Vysoká škola logistiky o.p.s.

Zabezpečení služeb uživatelů komunikačního uzlu

(Diplomová práce)

Přerov 2019 Bc. Vladimír Hubáček

Vysoká škola logistiky o.p.s.

Zadání diplomové práce

student	**Bc. Vladimír Hubáček**
studijní program	Logistika
obor	Logistika

Vedoucí Katedry magisterského studia Vám ve smyslu čl. 22 Studijního a zkušebního řádu Vysoké školy logistiky o.p.s. pro studium v navazujícím magisterském studijním programu určuje tuto diplomovou práci:

Název tématu: **Zabezpečení služeb uživatelů komunikačního uzlu**

Cíl práce:

Na základě návrhu výstavby a provozu komunikačního uzlu navrhnout provozní režimy komunikačního uzlu v podmínkách odstraňování následků přírodních katastrof resp. humanitárních krizí. Na typových příkladech ukázat zajištění provozu, interoperabilitu a integraci služeb komunikačního uzlu do příslušných logistických procesů.

Zásady pro vypracování:

Využijte teoretických východisek oboru logistika. Čerpejte z literatury doporučené vedoucím práce a při zpracování práce postupujte v souladu s pokyny VŠLG a doporučeními vedoucího práce. Části práce využívající neveřejné informace uveďte v samostatné příloze.

Diplomovou práci zpracujte v těchto bodech:

Úvod
1. Logistické procesy odstraňování důsledků přírodních katastrof resp. humanitárních krizí
2. Dotčené struktury státní, veřejné i soukromé sféry
3. Požadavky na komunikační infrastrukturu
4. Návrh integrace komunikačních služeb do postkrizových logistických procesů
5. Zajištění provozu komunikačního uzlu

Závěr

Rozsah práce: 50 – 60 normostran textu

Seznam odborné literatury:

Gros, I., Barančík, I., Čujan, Z.: Velká kniha logistiky. VŠCHT Praha, 2018, ISBN 978-80-7080-952-5

Novotný, V.: Mobilní komunikační sítě a služby v all-IP prostředí. VUT v Brně 2014, ISBN 978-80-214-5129-2

Šimák, L.: Krízový manažment vo verejnej správe. FŠI ŽU Žilina, EDIS 2001, ISBN 80-88829-13-5

Vedoucí diplomové práce: doc. Dr. Ing. Oldřich Kodym

Datum zadání diplomové práce: 31. 10. 2018
Datum odevzdání diplomové práce: 11. 5. 2019

Přerov 31. 10. 2018

doc. Dr. Ing. Oldřich Kodym
vedoucí katedry

doc. Ing. Ivan Hlavoň, CSc.
rektor

Čestné prohlášení

Prohlašuji, že předložená bakalářská/diplomová práce je původní a že jsem ji vypracoval/a samostatně. Prohlašuji, že citace použitých pramenů je úplná a že jsem v práci neporušil/a autorská práva ve smyslu zákona č. 121/2000 Sb., o autorském právu, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.

Prohlašuji, že jsem byl/a také seznámen/a s tím, že se na mou bakalářskou/diplomovou práci plně vztahuje zákon č. 121/2000 Sb., o právu autorském, právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména § 60 – školní dílo. Beru na vědomí, že Vysoká škola logistiky o.p.s. nezasahuje do mých autorských práv užitím mé bakalářské/diplomové práce pro pedagogické, vědecké a prezentační účely školy. Užiji-li svou bakalářskou/diplomovou práci nebo poskytnu-li licenci k jejímu využití, jsem si vědom/a povinnosti informovat před tím o této skutečnosti Vysokou školu logistiky o.p.s. prorektora pro vzdělávání.

Prohlašuji, že jsem byl/a poučen/a o tom, že bakalářská/diplomová práce je veřejná ve smyslu zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, zejména § 47b. Taktéž dávám souhlas Vysoké škole logistiky o.p.s. ke zpřístupnění mnou zpracované bakalářské/diplomové práce v její tištěné i elektronické verzi. Souhlasím s případným použitím této práce Vysokou školou logistiky o.p.s. pro pedagogické, vědecké a prezentační účely.

Prohlašuji, že odevzdaná tištěná verze bakalářské/diplomové práce, elektronická verze na odevzdaném optickém médiu a verze nahraná do informačního systému jsou totožné.

V Přerově dne 15. 8. 2019 …….

podpis

Poděkování

Děkuji všem, kdo svou radou nebo jinou pomocí přispěli k vytvoření této práce.

Název tématu: Zabezpečení služeb uživatelů komunikačního uzlu

Cíl práce: Na základě návrhu výstavby a provozu komunikačního uzlu navrhnout provozní režimy komunikačního uzlu v podmínkách odstraňování následků přírodních katastrof resp. humanitárních krizí. Na typových příkladech ukázat zajištění provozu, interoperabilitu a integraci služeb komunikačního uzlu do příslušných logistických procesů.

Title: Providing Services for the Users of a Communication Hub

Thesis Aim: Based on the design and operation of a communication hub, the aim of the thesis is to establish operating modes of the communication hub in natural disaster or humanitarian emergency relief missions. The thesis presents model examples demonstrating the operation, interoperability, and integration of the communication hub services into the relevant logistics processes.

OBSAH

ÚVOD

Cílem předložené diplomové práce je po teoretickém rozboru současné problematiky připravenosti IZS na krizové scénáře najít vhodné řešení pro návrh komunikačního centra, které může být nasazeno v ohnisku krizové situace jako kvalitní a spolehlivé řešení pro možnost komunikace s vnějším okolím. Vybranými komunikačními prostředky můžeme oboustranně z místa a na místo dění katastrofického scénáře přenášet živě potřebné informace, úkoly, pokyny a jiné formy dat pro východisko k řešení mimořádných událostí. Pomocí zasazení komunikačního uzlu do výbavy Integrovaného záchranného systému ČR (dále jen IZS) můžeme ještě více zefektivnit práci a záchrannou činnost příslušníků záchranných sborů, kteří s plným nasazením bojují o každou vteřinu pro záchranu lidských životů. Pomocí komunikačního uzlu je možné zvýšit informovanost nejen záchranných týmů, ale také civilního obyvatelstva v poškozené oblasti. Navíc díky technologiím dalekého dosahu se zde nabízí i možnost nasazení na území jiného státu, teoreticky kdekoli na světě, a poskytnutí humanitární pomoci v cizí zemi.

IZS, který je určen pro pomoc lidem v nouzi a je placen z daní občanů, by neměl zaostávat po technologické stránce, naopak by v tomto směru měly být nasazeny nejmodernější komunikační a informační prostředky pro potřebná kritéria datového přenosu jako jsou rychlost, spolehlivost, jednoduchost a nasaditelnost tak, aby krizová situace mohla být efektivně vyřešena.

Diplomová práce je členěna do pěti kapitol, z nichž první tři kapitoly jsou teoretickou částí práce, kde čtenáře podrobně seznamuji s problematikou komunikačních a informačních technologií a jejich zasazení v IZS. V samotné čtvrté kapitole se velmi podrobně věnuji samotnému návrhu komunikačního uzlu v různých provedeních pro národní, oblastní a lokální úroveň nasazení a využití služeb. Pátá kapitola je zaměřena zejména na provoz a interoperabilitu komunikačního centra v době nasazení.

Pro téma práce tohoto zaměření jsem se rozhodl, protože jsem již delší dobu zaměstnancem Ministerstva obrany ČR, konkrétně náčelníkem skupiny, která zajišťuje prostředky komunikačních a informačních technologií a vím, že nasazení vhodného funkčního a kompaktního komunikačního uzlu v rámci IZS chybí. Cílem práce není systém jakkoli hodnotit, nýbrž nalézt řešení, které jej vylepší zejména v komunikační oblasti a zjednoduší tak zvládání krizové situace.

1 LOGISTICKÉ PROCESY ODSTRAŇOVÁNÍ DŮSLEDKŮ PŘÍRODNÍCH KATASTROF A HUMANITÁRNÍCH KRIZÍ

1.1 Humanitární krize a ČR

Poskytování humanitární pomoci ČR se řídí zákonem č. 151/2010 Sb., o zahraniční rozvojové spolupráci a humanitární pomoci poskytované do zahraničí. Humanitární pomoc poskytovaná do zahraničí je souhrn činností hrazených ze státního rozpočtu, jejichž cílem je zamezit ztrátám na životech a újmě na zdraví, zmírnit utrpení a obnovit základní životní podmínky lidí po vzniku mimořádných událostí, jakož i zmírňovat dlouhodobě trvající následky mimořádných událostí a předcházet jejich vzniku a negativním následkům.

Humanitární pomoc zahrnuje jak reakci na ad-hoc přírodní či lidmi způsobené katastrofy, tak pomoc v dlouhodobých (komplexních) humanitárních krizích a při prevenci katastrof [1].

1.1.1 Pojetí mimořádných situací

Termín **mimořádná situace** nachází využití všude tam, kde je v návaznosti na neobvyklost a mimořádnost nastávající nebo již nastalé situace zapotřebí uplatnit postupy krizového managementu v rozpětí od diagnostikování situace a analýzy možného vývoje, přes krizové rozhodování až po realizační krizové postupy a v jejich rámci příslušná opatření.

Sofistikovaný přístup ke zvládání krizí je natolik zásadní, že si termín krizová situace a její zvládání zasluhuje objasnění i z teoretického hlediska.

V profesionální praxi krizového řízení bývá krizová situace vnímána jako situace mimořádná, znamenající různě intenzivní, ale vždy značný rozsah ohrožení hodnot – životů, zdraví, majetku a životního prostředí – projevující se na konkrétním území a na určitém stupni veřejné správy. Rozdílná intenzita a velikost možných ohrožení vede k úvahám, zda se krizová situace vymezuje dostatečně vůči tzv. „běžné“ mimořádné události nepříliš závažného dosahu, v čem podstata odlišení, a zda vysvětlení pojmů „krizová situace“ a „mimořádná událost“ není v právních normách krizového řízení

poněkud ošizeno. K objasnění významu uvedených pojmů příliš nepomůže ani jejich vymezení v anglickém originále, kde se můžeme setkat s pojmy *accident* (nehoda), *emergency* (mimořádná událost), *disaster* (pohroma, neštěstí, havárie ad.) a *crisis* (krize) – viz také [2], [3].

1.1.2 Korelace mimořádných událostí a krizových situací

Mimořádná událost i krizová situace má řadu přívlastků a více či méně výstižných příměrů, které vyjadřují, co je mimořádná událost a co krizová situace. Potud může být navozeno zdání, že to pro praxi postačuje. Co však zcela jistě praxi schází, je dostatečné vyjádření souvztažnosti mezi nimi. Tento deficit omezuje zhodnocení reálných ohrožení v různých měřítcích (územních, časových) a potažmo brání i optimálním reakcím na tato ohrožení.

Podle ustanovení § 2 písm. b) zákona č. 239/2000 Sb., o integrovaném záchranném systému a o změně některých zákonů, ve znění pozdějších předpisů, se pro účely tohoto zákona rozumí „mimořádnou událostí škodlivé působení sil a jevů vyvolaných činností člověka, přírodními vlivy, a také havárie, které ohrožují život, zdraví, majetek nebo životní prostředí a vyžadují provedení záchranných a likvidačních prací“. Naproti tomu se podle ustanovení § 2 písm. b) zákona 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů, pro účely tohoto zákona rozumí „krizovou situací mimořádná událost, při níž je vyhlášen stav nebezpečí nebo nouzový stav nebo stav ohrožení státu“. Na první pohled je zřejmé, že definice krizové situace tohoto znění je výrok poněkud zjednodušený.

Do jeho obsahu se vešlo pouze vyhlášení krizového stavu coby administrativního aktu, i když podmíněného příslušnou pravomocí rozhodování. Svázání krizové situace s krizovým stavem v tomto znění odpovídá právním souvislostem zákona, tedy potřebám práva, nicméně neodpovídá faktickému pojetí krizové situace samotné. Zde jednoznačně vychází, že krizová situace musí být vztažena ke stupni a předpokládaným dopadům mimořádné události a musí mít zcela charakteristický průběh [3].

1.1.3 Krizové jevy a krizová situace

Výskyt krizových jevů dává vždy určitý obraz krizové situace (zjednodušeně krize). Z analogie o chování systémů víme, že při vybočení kteréhokoli prvku prostředí ze stability se tento prvek jeví jako nestabilní a stává se možným zdrojem nestability

tohoto prostředí. Četnost a míra nestability prvků může narůstat, až dosáhne hranice, při níž přestává být prostředí stabilní a stává se nestabilním. To znamená, že za krizi nejčastěji považujeme kritickou situaci (situaci ve spojitosti s krizovými jevy), kdy v určitém prostředí dojde k nahromadění negativních, pro krizi příznačných jevů nestability, jež znemožňují řádné fungování určité oblasti infrastruktury a vyžadují zásadní řešení.

Vidění krize v dynamice změn podtrhuje „slovník cizích slov“, kde je krize popsána jako vyvrcholení, rozhodná chvíle, obrat ve vývoji nebo nebezpečný stav vývoje [3].

Vývojový cyklus krize je popsán v příloze č. 1.

1.1.4 Přínos porozumění termínu krizová situace

Porozumění termínu krizová situace má svá praktická uplatnění, zejména:

- pomáhá posuzovat mimořádnou událost, krizovou situaci a krizový stav podle určitých pravidel;
- přináší odpověď, jak reakce na vznik a průběh krizové situace souvisí s činností zásahových složek a orgánů krizového řízení a jak průběh krizové situace odráží samostatnost i fúzi jejich působnosti (v hranicích mimořádná událost – krizová situace);
- podporuje dovednosti tvořit operační plány pro konkrétní krizové situace, jako součást krizového plánu;
- přispívá lektorování většiny odborných pojednání o krizových situacích [3].

1.1.5 Příprava na potenciální krize a havarijní plánování

Plnění povinností podniku v oblasti řízení rizik, prevence nehod a BOZP[1] nelze zajistit bez dobře zorganizovaného **bezpečnostního managementu.** Fungující bezpečnostní management je zároveň předpokladem pro identifikaci a včasnou nápravu negativních provozních faktorů, rozhodujících o kvalitě, produktivitě a ekonomičnosti provozu.

Ve vyspělých zemích a firmách stojí bezpečnost práce na nejvyšším stupni v hierarchii podnikových priorit. Odstraňování všech činitelů, které by mohly ohrozit zdraví zaměstnanců, je věnována soustavná péče. Velký důkaz je kladen na dodržování pravidel bezpečného chování každým pracovníkem. V některých podnicích se např.

[1] **BOZP→** bezpečnost a ochrana zdraví při práci

upustilo od odměňování podle výkonu a jako rozhodující kritérium pro rozdělování nadstandardních mzdových prostředků je používáno právě bezpečné jednání. Prvním očividným důsledkem, kterého si zde každý musí všimnout, je zásadní změna způsobu, jak lidé o své práci uvažují, jaké postoje a hodnoty převládají, jaká úroveň pracovní disciplíny se zde stala normálním standardem.

Manažeři, kteří ve svém rozhodování opomíjí úzkou souvislost mezi pracovními podmínkami (v širokém významu tohoto pojmu) a produktivitou práce, zpravidla podceňují celou problematiku spolehlivosti lidského činitele. Bezpečnostními otázkami se zabývají, až když se něco závažného stane, a neuvědomují si, jak velký dopad může mít projevovaný nezájem o odstraňování nepříznivých, stresujících a ohrožujících faktorů na pracovní iniciativu a disciplínu zaměstnanců. Dokonce si někdy nepřipouštějí ani svou trestněprávní odpovědnost. Prevenci rizik považují za určitý přepych (protože frekvence úrazů v jejich podniku nevybočuje příliš z průměru) a nechtějí vidět mnohokrát potvrzenou skutečnost, že následné ekonomické ztráty zpravidla značně převyšují náklady na prevenci [5, s. 372, 373].

Havarijní plánování:

- je komplex opatření, vytvářející havarijní připravenost regionu (oblasti, okresu, obce) nebo subjektu k řešení mimořádných událostí (dále jen „MU“, vzniklých v důsledku technických a technologických havárií, ale i v důsledku působení přírodních živlů a následnému vzniku těchto havárií,
- havarijní připraveností se rozumí příprava opatření na odvrácení dopadů havárií nebo alespoň na jejich zmírnění (zahrnuje zpracování scénářů možných závažných havárií, odezvy na možné závažné havárie, řízení odezvy na možné závažné havárie, přípravu prostředků a pomůcek nutných pro odezvu na závažné havárie),
- je soubor činností, postupů a vazeb uskutečňovanými ministerstvy a jinými správními úřady, dotčenými právnickými nebo podnikajícími fyzickými osobami k plánování opatření na provádění záchranných a likvidačních prací při vzniku MU, a to vždy s použitím dosažitelných sil a prostředků.

Cílem havarijního plánování je:

- zvýšit uvědomění si možných rizik a provedení jejich analýzy (analýza rizik),
- minimalizovat škodlivé účinky MU na životy a zdraví osob, životní prostředí, hospodářská zvířata, majetkové a kulturní hodnoty,

- stanovit opatření k odvrácení nebo omezení účinků MU a způsob odstranění následků vazbami součástí krizového plánování,

Místo a úloha havarijního plánování v návaznosti na vývoj MU je uvedena na obrázku v příloze č. 3.

Výsledkem havarijního plánování jsou **havarijní plány**, které lze rozdělit takto:

- havarijní plány objektové,
- vnitřní havarijní plány,
- havarijní plány vodního hospodářství a ochrany vod před závadnými látkami,
- havarijní plány ochrany ovzduší pro případy poruch a nehod u technických zařízení,
- havarijní plány k předcházení vzniku a k řešení stavů nouze v energetickém sektoru,
- havarijní plány územní, které jsou přílohou krizového plánu kraje,
- havarijní plán kraje,
- vnější havarijní plány,

V případě, že rozsah MU je takového rozsahu a záchranné a likvidační práce je třeba koordinovat na strategické úrovni, je vyhlašován zvláštní stupeň poplachu územně příslušného poplachového plánu (MU přerůstá do krizové situace) a může být příslušným orgánem krizového řízení vyhlášen krizový stav.

V případě vyhlášení krizového stavu je krizová situace řešena v režimu krizového řízení s využitím předem zpracovaných krizových plánů [6].

1.2 Doprava jako důležitý logistický proces pro likvidaci škod

Pro řešení humanitární krize jsou důležité správně nastavené logistické procesy, které souvisejí s efektivní likvidací škod a s humanitární pomocí. Důležitým logistickým procesem v krizovém plánování je doprava potřebného matriálu do postižené lokality ve správný čas.

1.2.1 Druhy dopravních systémů

Z technického hlediska lze rozdělit dopravní systém, označovaný také jako **dopravní infrastruktura**, na dvě hlavní části:

- **síť dopravních cest** spolu s dalšími obslužnými objekty,

- **dopravní prostředky**, které se na sítích pohybují.[2]

Ze systémového hlediska tvoří obě části množinu prvků dopravního systému. Podle jejich uspořádání, používané technologie a provedení je lze rozdělit na systémy silniční, železniční, říční, námořní, potrubní, letecké a lanové (kabelové) dopravy. Jejich stručná charakteristika je v tabulce v příloze č. 4. Stranou ponecháme historicky nejstarší dopravu využívající síly zvířat, používanou v současné době jen omezeně např. při stahovaní dřeva z obtížně přístupných míst, a dopravu prostřednictvím lidské síly na krátké vzdálenosti, např. manipulace s materiálem ve skladovacích systémech.
K základním charakteristikám determinujícím jejich použití patří:

- **rychlost –** vyjadřující jak rychle lze zboží dopravit z výchozí do koncové destinace,
- **dostupnost –** určující kam všude lze zboží dopravit,
- **spolehlivost –** daná pravděpodobností, že dopravíme zboží nebo osoby včas na požadované místo,
- **univerzálnost** – výčet všeho, co lze daným dopravním prostředkem dopravit do požadovaného místa,
- **frekvence** – schopnost opakovat přepravní výkony, jak často lze zboží dopravovat v daném období,
- **stoupavost** – schopnost překonávat převýšení mezi výchozími a cílovými destinacemi,
- **náklady –** za kolik je možno požadovaný náklad dopravit,
- **ekologická zátěž** – vliv výkonu přepravních činností na životní prostředí [7].

1.2.2 Doprava a přeprava v krizovém řízení a ochraně obyvatelstva

Dopravní a přepravní systémy mají v logistice důležitou roli. Doprava nejen umožňuje propojení jednotlivých částí logistického procesu, tj. vytváření logistických řetězců, ale může také napomoci logistice při řešení míst styku mezi jednotlivými subsystémy logistického procesu. Zajištění přepravy zahrnuje výběr způsobu přepravy (např. letecké, železniční, nákladní, automobilové), výběr přepravní trasy, zajištění toho, aby nebyly překročeny předpisy země, kde doprava probíhá a konečně výběr dopravce.

[2] Zřídka je používán pojem dopravní infrastruktura jen pro označení sítě cest.

V rámci krizového řízení a ochrany obyvatelstva dochází k přesunu **materiálu, zboží** a **osob**. V případě materiálu a zboží se může jednat o přesun z místa vzniku do místa spotřeby. Jako příklad může sloužit přeprava pohotovostních zásoba zásob pro humanitární pomoc ze skladů Správy státních hmotných rezerv směrem k postiženému obyvatelstvu prostřednictvím nákladní dopravy. Přepravou osob se v krizovém řízení a ochraně obyvatelstva rozumí přesun osob (např. policisté, hasiči, starosta obce) za účelem plnění úkolů, které jim vyplývají z jejich povolání nebo ze zákona. Příkladem může být přesun policistů a hasičů do místa, kde probíhá evakuace osob v souvislosti s krizovou situací. Policisté a hasiči mohou k tomuto přesunu využít vlastních dopravních prostředků nebo služeb externích dopravců.

Veřejná správa si ve většině případů různé druhy přepravy objednává u externích dopravců. Výběr vhodného a spolehlivého dopravce je důležitý vzhledem k různorodosti přepravovaného zboží a potřebě doručit požadované zboží ve správném čase na správné místo – viz také [8], [9].

1.3 Logistika a logistická podpora v krizovém řízení a ochraně obyvatelstva

Logistika zahrnuje organizaci, plánování a řízení materiálního, finančního a informačního toku. Úkolem je zajistit, aby bylo správné zboží ve správném čase, ve správném množství, ve správné kvalitě a se správnými náklady na správném místě tak, aby došlo k uspokojení požadavků zákazníka. Logistiku a logistickou podporu v krizovém řízení a ochraně obyvatelstva je možné přirovnat k logistice v ostatních odvětvích lidské činnosti. Hlavním cílem logistiky je vždy uspokojení požadavků zákazníka. V následujících kapitolách jsou popsány vybrané logistické činnosti ve vztahu ke krizovému řízení a ochraně obyvatelstva. Dále jsou zde uvedeny základní informace k Institutu ochrany obyvatelstva, Základně logistiky Olomouc, Správě státních hmotných rezerv ČR a Hasičskému záchrannému sboru České republiky.

Nutno také v této problematice zmínit **zákaznický servis v krizovém řízení a ochraně obyvatelstva**, což je poskytování služeb pro zákazníky před, během a po nákupu. Zákazníka, je možno definovat jako osobu, firmu, nebo jiný subjekt, který nakupuje zboží a služby vyrobené jinou osobou, firmou nebo jiným subjektem. Poskytování

služeb před, během a po, lze v krizovém řízení a ochranně obyvatelstva chápat následovně:

- **služby před** - preventivní opatření, plánování, součinnostní cvičení složek integrovaného záchranného systému atd.,
- **služby během** - provádění záchranných prací, evakuace, varování atd.,
- **služby po** - likvidační práce, obnovovací práce atd.

Jako zákazníka si v krizovém řízení představíme zejména vládu České republiky, ministerstva a jiné správní úřady, Českou národní banku, orgány kraje a ostatní orgány s územní působností a orgány obce. V případě ochrany obyvatelstva si jako zákazníka můžeme představit jednotlivé složky integrovaného záchranného systému, zejména Hasičský záchranný sbor České republiky. V souvislosti s krizovým řízením a ochranou obyvatelstva nesmíme zapomenout na občana, který je pravděpodobně nejdůležitějším zákazníkem v rámci krizového řízení a ochrany obyvatelstva. Role zákazníka se může v krizovém řízení i ochraně obyvatelstva měnit a to v závislosti na stupni řízení. Orgány obce se tak mohou stát zákazníkem ve vztahu k orgánům kraje. Toto platí také pro občana. Ten může být vyzván k poskytnutí osobní nebo věcné pomoci. Všichni výše uvedení zákazníci musí vždy požadovat, aby dodání výrobků, prací a služeb a všech procesů s nimi souvisejících bylo na nejvyšší úrovni a to jak v době před, v průběhu a po opatřeních, které byly přijaty v souvislosti s ochranou obyvatelstva a krizovou situací. Je třeba mít na paměti, že jde zejména o ochranu života, zdraví, majetku a životního prostředí a občané budou po právu ti nejnáročnější zákazníci, kteří budou požadovat provedení preventivních, záchranných, likvidačních a obnovovacích prací ve stoprocentní kvalitě. Podle mého názoru jsou si orgány krizového řízení a ochrany obyvatelstva své role v zákaznickém servisu ve vztahu k občanovi vědomí [10].

1.3.1 Plánování v krizovém řízení a ochraně obyvatelstva

Plánování je obecně činnost, při které se vytvářejí podklady pro rozhodování v současné době i v budoucnosti. Plánování je uvědomělá činnost řídících subjektů, která spočívá ve volbě a předpokládání cílů, úkolů, variant a způsobů, které podmiňují dosažení těchto cílů. Za nejdůležitější rys plánování se považuje volba cíle. Plánování není sestavení hierarchického souboru příkazů, které se mají bezmyšlenkovitě plnit. Je to tvůrčí činnost, která má stanovit reálný cíl a určit nejvýhodnější způsob jeho dosažení. K dosažení dlouhodobých cílů se používá strategické plánování a pro dosažení

krátkodobých cílů plánování operativní. V případě logistického zabezpečení krizového řízení a ochrany obyvatelstva je nutné shromáždit co nejpřesnější informace k sestavení požadavků na materiál, výrobky a služby, které jsou potřeba k zabezpečení fungování všech složek podílejících se na krizovém řízení a ochraně obyvatelstva. Potřebné informace jsou získávány na základě různých analýz, např. analýzy rizik a analýzy území, které jsou součástí havarijních a krizových plánů. Na základě získaných výsledků jsou následně vytvářeny požadavky na prostředky, které jsou nezbytné k zajištění fungování veřejné správy, zasahujících složek a k uspokojení potřeb občanů [10].

1.3.2 Doprava a přeprava v krizovém řízení a ochraně obyvatelstva

Dopravní a přepravní systémy mají v logistice důležitou roli. Doprava nejen umožňuje propojení jednotlivých částí logistického procesu, tj. vytváření logistických řetězců, ale může také napomoci logistice při řešení míst styku mezi jednotlivými subsystémy logistického procesu [8]. Zajištění přepravy zahrnuje výběr způsobu přepravy (např. letecké, železniční, nákladní, automobilové), výběr přepravní trasy, zajištění toho, aby nebyly překročeny předpisy země, kde doprava probíhá a konečně výběr dopravce [9].
V rámci krizového řízení a ochrany obyvatelstva dochází k přesunu **materiálu, zboží** a **osob**. V případě materiálu a zboží se může jednat o přesun z místa vzniku nebo skladování do místa spotřeby. Jako příklad může sloužit přeprava pohotovostních zásob a zásob pro humanitární pomoc ze skladů Správy státních hmotných rezerv směrem k postiženému obyvatelstvu prostřednictvím nákladní dopravy. Přepravou osob se v krizovém řízení a ochraně obyvatelstva rozumí přesun osob (např. policisté, hasiči, starosta obce) za účelem plnění úkolů, které vyplývají z jejich povolání nebo ze zákona. Příkladem může být přesun policistů a hasičů do místa, kde probíhá evakuace osob v souvislosti s krizovou situací. Policisté a hasiči mohou k tomuto přesunu využít vlastních dopravních prostředků nebo služeb externích dopravců.
Veřejná správa si ve většině případů různé druhy přepravy objednává u externích dopravců. Výběr vhodného a spolehlivého dopravce je důležitý vzhledem k různorodosti přepravovaného zboží a potřebě doručit požadované zboží ve správném čase na správné místo – viz také [8], [9].

1.3.3 Správa státních hmotných rezerv

Správa státních hmotných rezerv je ústředním orgánem státní správy pro hospodářská opatření v krizových situacích a pro státní hmotné rezervy.

Správa státních hmotných rezerv zabezpečuje financování, obměnu, záměnu, půjčku, uvolnění, nájem, prodej, skladování, ochraňování a kontrolu státních hmotných rezerv a podle požadavků krizových plánů i jejich pořizování.

Státní hmotné rezervy se z hlediska účelu člení na:

a) **Hmotné rezervy** - tvoří vybrané základní suroviny, materiály, polotovary a výrobky. Jsou určeny pro zajištění obranyschopnosti a obrany státu, pro odstraňování následků krizových situací a pro ochranu životně důležitých hospodářských zájmů státu.

b) **Mobilizační rezervy** - tvoří vybrané základní suroviny, materiály, polotovary, výrobky, stroje a jiné majetkové hodnoty určené pro zajišťování mobilizačních dodávek.

c) **Pohotovostní zásoby** - tvoří vybrané základní materiály a výrobky, určené k zajištění nezbytných dodávek pro podporu obyvatelstva, činnosti havarijních služeb a hasičských záchranných sborů po vyhlášení krizových stavů, v systému nouzového hospodářství, kterou nelze zajistit obvyklým způsobem.

d) **Zásoby pro humanitární pomoc** - tvoří vybrané základní materiály a výrobky určené po vyhlášení krizových stavů k bezplatnému poskytnutí fyzické osobě vážně materiálně postižené.

Hmotné rezervy jsou tvořeny zejména ropou a ropnými produkty. Mobilizační rezervy a pohotovostní zásoby jsou určeny pro řešení různých typů krizových situací. V současné době nabývá na významu materiální zabezpečení pro řešení nevojenských krizových situací. Správa státních hmotných rezerv se zpravidla podílí na řešení velkých krizových situací až v okamžiku vyhlášení nouzového stavu. Připravenost a perfektně fungující zázemí jsou v takové situaci nezbytným předpokladem jejího úspěšného a včasného řešení, které zabrání zbytečným škodám na majetku, zdraví a životech spoluobčanů [10].

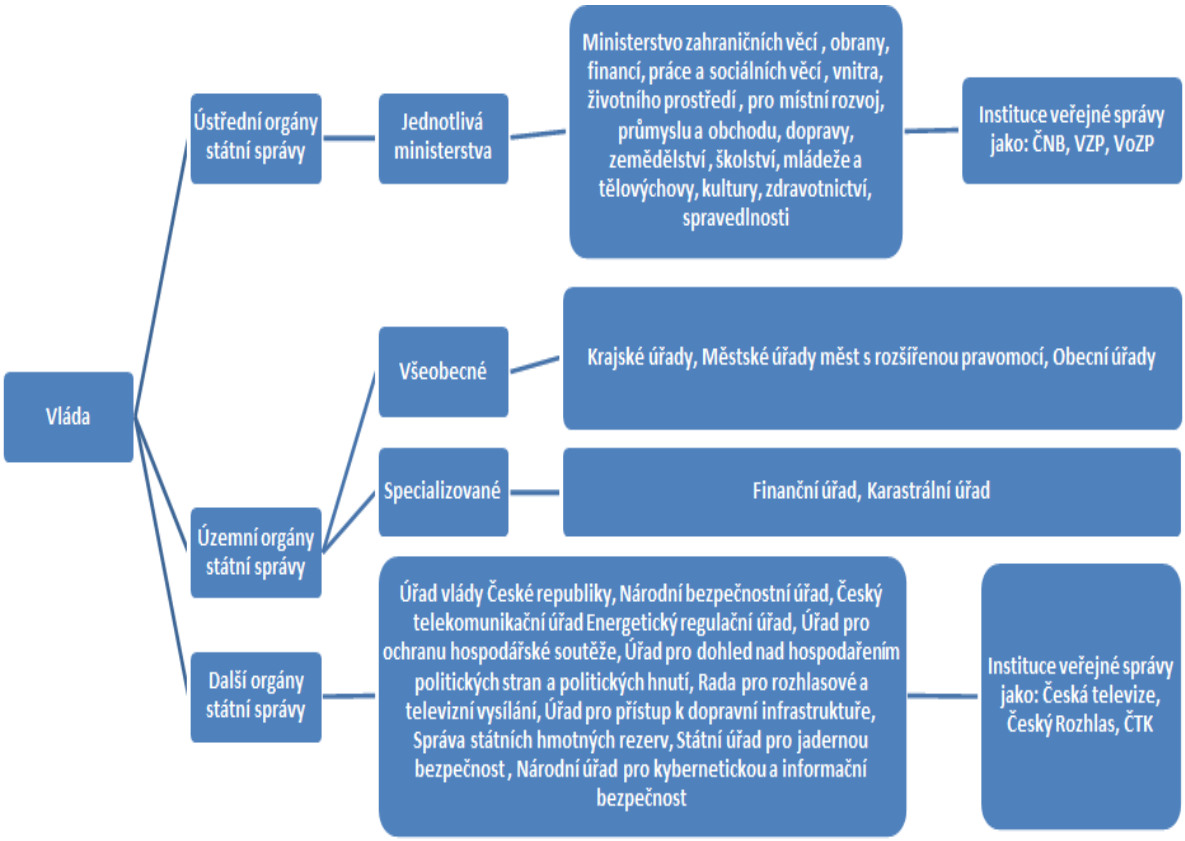
Vojenská logistika je dle definice NATO naukou „*o plánování, provádění přesunu a technickém zabezpečení sil. Klade praktický důraz na aktivizaci zdrojů, tj. na vytvoření a udržovaní normovaných zásob vojenského materiálu z dodávek výrobců a na operační bázi, tj. na rychlé a hospodárné přemístění materiálu do míst využití“*. Tuto definici lze podle mého názoru použít s malými změnami také pro logistiku

a logistickou podporu v krizovém řízení a ochraně obyvatelstva. Dobře fungující logistika a logistická podpora v krizovém řízení a ochraně obyvatelstva je klíčem k efektivní ochraně obyvatel, zvířat, majetku a životního prostředí. Je třeba mít na paměti, že každá chyba v logistickém řetězci může vést ke značným škodám. Chyby by měly být odhalovány především při pravidelných součinnostních cvičeních složek integrovaného záchranného systému a orgánů krizového řízení. Cvičení by měla být do poslední chvíle utajena před zasahujícími složkami a měla by vycházet z reálných situací, které mohou v běžném životě člověka nastat. Chyby, v jejichž důsledku dojde k ohrožení nebo ke ztrátě lidského života, jsou nepřípustné [10].

2 DOTČENÉ STRUKTURY STÁTNÍ, VEŘEJNÉ ISOUKROMÉ SFÉRY

Jakákoliv vzniklá krize zasahuje všechny stupně státní a veřejné sféry – viz obrázek 2.1. V běžně rozvinutých státních zřízeních jsou to ústřední orgány státní správy, územní orgány státní správy. V rámci veřejné správy jsou to zejména instituce s právní subjektivitou. V případě soukromé sféry se jedná o právnické osoby, které mají se statutárními orgány tedy s potencionálními krizovými štáby uzavřenou dohodu o případném využití movitého i nemovitého majetku pro stabilizaci krizového scénáře. V některých případech (mobilizace, ohrožení bezpečnosti státu) je možno zabavit majetek právnických osob pro účely řešení krizových situací i bez jakékoli dohody – viz zákon č. 430/2010 Sb., který upravuje původní zákon č. 240/2000 Sb. o krizovém řízení.

Obr. 2.1 Rozdělení stupňů státní a veřejné správy



Zdroj: vlastní zpracování

2.1 Možné role organizací v případě krizového scénáře

Případná krize zasahuje do činnosti všech oblastí běžného života občanů a státního uspořádání na všech úrovních společnosti. V případě ekonomicky silné společnosti s jasným státním nebo mocenským uspořádáním a fungující státní a veřejnou správou je jedním z důležitých prvků připravenost na možný příchod krize. V případě státu s nejasným státním uspořádáním nebo slabou ekonomickou výkonností je vypořádání s krizovým stavem výrazně těžší, zejména s ohledem na krizové řízení.

Státní správa

Ústředním orgánem státní správy je celostátní krizový štáb a jeho poradním a výkonným orgánem jsou vzhledem k jejich celostátní působnosti především jednotlivá ministerstva. Z pohledu logistických procesů je základním prvkem státní správy využitým při krizovém řízení Integrovaný záchranný systém a jeho jednotlivé prvky.
Územní orgány státní správy jsou zejména krajské úřady a jejich krizové štáby krajů a na nižších úrovních jsou to krizové štáby obcí s rozšířenou pravomocí a krizové štáby obcí. V ČR je organizační uspořádání krizových štábů řešeno směrnicí ministerstva vnitra č. j. MV-117572-2/PO-OKR-2011 ze dne 24. listopadu 2011. V rámci logistických procesů jsou na jednotlivých úrovních územních orgánů státní správy nasazovány primárně hotovostní jednotky Integrovaného záchranného systému, které spadají pod jednotlivé správní celky. Jsou to obecní a městská policie, technické služby, služby správy sociálního zabezpečení.

Veřejná správa

Základní institucí, která z logistického pohledu nejvíce vystupuje do popředí zájmu, je v případě jakékoliv krize Správa státních hmotných rezerv, kterou je v různých formách začleněna v rámci veřejné správy v každé zemi. Úlohou takové organizace je přijímat zejména hospodářská opatření pro krizové stavy a zajišťovat státní hmotné rezervy. Dále zajišťuje i koordinaci věcných zdrojů za krizových situací a po vyhlášení krizových stavů. K tomu vytvořila a provozuje informační systémy pro podporu plánovacích a rozhodovacích procesů orgánů krizového řízení [11].

Mezi státní hmotné rezervy lze řadit tyto:

- **Hmotné rezervy** - základní suroviny, materiály, polotovary a výrobky. Jsou určené pro zajištění obranyschopnosti a obrany státu a pro odstraňování následků krizových situací.
- **Mobilizační rezervy** - k nim patří i stroje a majetkové hodnoty, které jsou určené pro zajišťování mobilizačních dodávek.
- **Pohotovostní zásoby** - základní materiály a výrobky, určené k zajištění nezbytných dodávek pro podporu obyvatelstva, činnosti havarijních služeb a hasičských záchranných sborů po vyhlášení krizových stavů, v systému nouzového hospodářství, kterou nelze zajistit obvyklým způsobem, a pro materiální humanitární pomoc poskytovanou do zahraničí.
- **Zásoby pro humanitární pomoc** - základní materiály a výrobky určené po vyhlášení krizových stavů k bezplatnému poskytnutí fyzické osobě vážně materiálně postižené.

Další výrazně zasažené instituce veřejné správy jsou zejména státní zdravotní pojišťovny, státní radiokomunikace. Státní finanční instituce včetně Národní banky.
Humanitární krize zasahuje do všech oblastí soukromé sféry. Výrazně ovlivňuje výrobu, obchod i služby a to ve všech odvětvích.
V této části práce a v návaznosti na další fakta, která jsou uvedená níže, považuje autor za vhodné uvést skutečnost, že mezi důležité aspekty výchozí situace pro řešení jakéhokoliv katastrofického scénáře nebo krizové události je potřeba učinit potřebné kroky k okamžitému zahájení **humanitární činnosti**, potažmo **pomoci**. Touto problematikou se budeme zabývat do hloubky v následujících kapitolách [11].

2.2 Důvody vedoucí k humanitární činnosti

Obecně jsou rozlišovány tři druhy krizí, během kterých dochází k humanitární intervenci:

- **Přírodní katastrofy** (zemětřesení, záplavy, sucho, hurikány atd.)
  Jedná se o náhlou událost, tzv. ad hoc katastrofu, jejíž šíře je dána velikostí zasaženého území, počtem mrtvých, raněných a velmi často i dlouhodobě se

pohřešujících lidí. Obecně je také charakterizována vysokým stupněm materiálních škod.

- **Krize zaviněné člověkem** (války, lokální konflikty, ozbrojené incidenty atd.) Charakteristickým znakem krizí zaviněných člověkem, mysleme jeho chováním a konáním, bývá často stěhování civilistů z nebezpečných zón konfliktu. Velmi často se o těchto krizích doslýcháme z jihozápadní části Asie. Více než při jiném druhu krize by se měl právě zde zdůraznit význam mezinárodního humanitárního práva a s ním spojeného i uprchlického práva. Na tomto místě je nutné připomenout dodržování principu nestrannosti a nezávislosti při každé humanitární akci.
- **Strukturální krize** (politické, ekonomické nebo sociální) Se strukturální krizí je úzce spojován pojem „komplexní politická krize“. Ta nastává tehdy, pokud humanitární krizi doprovází i jiné nežádoucí vlivy, které pomoc značně znesnadňují. Ať už se jedná o politickou nestabilitu, selhání státu z pohledu organizace, špatné přírodní vlivy nebo neočekávané šíření epidemií. Z významu slov „strukturální“ a „komplexní“ lze vyvodit, že jde o krizi dlouhodobou, právě z důvodu interakce několika pro organizaci společnosti klíčových oblastí. Pro ilustraci bychom mohli uvést jako příklad větší část afrického kontinentu, dále země jako Súdán, Pákistán, Afghánistán a Somálsko. Do této skupiny můžeme bezpochyby také zařadit ostrov Haiti, kde rozvojová pomoc probíhala i před zemětřesením. Souhrnně se tyto země s podobnými charakteristikami nazývají „křehké země“. V zemích s komplexní humanitární krizí se nachází množství neziskových organizací, které v nich zabezpečují plánované dlouhodobé mise, častokrát společně s programy OSN [11].

Dle Ministerstva zahraničních věcí ČR lze vymezit tři na sebe navazující fáze pomoci, které se uplatňují při každé z výše zmíněných krizí.

Okamžitá pomoc

Nejkrizovější nejčastěji bývá první fáze, kdy humanitární pomoc začíná proudit v horizontu hodin, dnů i týdnů. Základní pomoc se soustřeďuje zvláště na záchranu životů lidí. Účelem je zajistit nezbytný zdravotní materiál, kvalifikované zdravotníky a jiné potřeby, které vyplývají z uvedeného třetího bodu deklarace Good Humanitarian Donorship. Podle závažnosti humanitární krize se na krizovém řízení často podílejí

i složky OSN, představující důležitý koordinační prvek. Prostřednictvím okamžité humanitární výzvy - „flash appealu“ - oznamuje OSN souhrn humanitárních potřeb, které si postižená země nemůže svými silami zajistit sama.

Rehabilitace

Fáze rehabilitace probíhá od druhého až třetího týdne po katastrofě a může trvat až po dobu tří měsíců. Kromě základních opatření, která se týkají okamžité pomoci, bývá dalším stanoveným cílem obnovení infrastruktury (například dopravních cest, elektřiny…). V tomto druhém období se také sčítají škody, vyhodnocují se celkové následky události. Údaje, které vzejdou z výsledných analýz, jsou důležité pro stanovení dalších priorit obnovování. Pro dosažení co nejefektivnější kooperace mezi různými týmy, rozdělenými dle jejich oblasti působnosti, se obvykle pořádají tzv. *clustery* neboli „pracovní porady“ zástupců týmů stejného zaměření, které jsou organizované Úřadem pro koordinaci humanitární pomoci (OCHA). Z hlediska struktury OCHA spadá pod OSN. V těchto týmech jsou většinou zastoupeny různé neziskové organizace, jejichž cílem je vzájemná souhra a neustálé předávání informací je považováno za nezbytnost.

Obnova a rozvoj

Poslední fáze - obnova a rozvoj - se vymezuje přibližně do dvou let od zahájení humanitární pomoci. Počítá se s obnovou poškozených či zcela zničených obydlí obyvatel. Velmi významnou složkou je znovuobnovení zdrojů obživy, kdy se lidé v zasažených oblastech učí například novým technikám pěstování plodin nebo stavebním dovednostem. Po všech neblahých okolnostech, kterými si země musela projít, ji tato fáze nabízí příležitost dosáhnout určitého stupně zlepšení celkových životních podmínek. Je to typické zejména pro málo rozvinuté země. Tento efekt se označuje anglickým termínem *„buildingbackbetter“*. Do obnovy je nutné zakomponovat i předcházení vážným následkům katastrofy, zvláště tam, kde dochází k opakujícím se krizím, což vyplývá i z deklarace, o které jsme pojednali výše [12].
Řízení humanitární pomoci a průběh humanitárních projektů v praxi je popsán v příloze č. 2.

3 POŽADAVKY NA KOMUNIKAČNÍ INFRASTRUKTURU

K úspěšnému zvládnutí krizového stavu je nezbytně nutná dostupná, funkční hlasová a datová komunikace na všech úrovních řízení a také mezi nimi. Jedním ze základních požadavků je rozdělení infrastruktury na veřejnou a neveřejnou část, kdy neveřejná část slouží zejména ke komunikaci na mezinárodní úrovni a v případě národní úrovně pouze v rámci vlády, její komunikace s ministerstvy a vybranými institucemi veřejné správy (Národní banka, Správa státních hmotných rezerv).

K tomuto rozdělení dochází zejména z důvodu zabezpečení sdílení utajovaných informací pouze v rámci osob oprávněných se s nimi seznamovat. Základními neveřejnými osobními údaji jsou pro občana jeho rodné číslo, krevní skupina, náboženské vyznání, zdravotní stav nebo třeba sexuální orientace. U institucí to jsou informace v širokém spektru dle jednotlivých odborných zaměření a to od finančního tajemství, listovního tajemství, lékařského tajemství až po utajované informace vojenského charakteru.

Požadavky tak můžeme rozdělit na mezinárodní a národní komunikace.

Komunikace mezinárodní

Tato infrastruktura zajišťuje možnost komunikace jednotlivých zúčastněných subjektů se zahraničím. Hlasovou, popř. datovou komunikaci pak můžeme případně rozdělit na **utajovanou** a **neutajovanou**.

Máme pak na mysli:

- Komunikace státní a veřejné správy s vnějším světem. Zde se jedná především o komunikaci vládních činitelů s organizacemi, jako jsou OSN, NATO nebo EU. V případě požadavku na finanční pomoc bude národní banka komunikovat s Mezinárodním měnovým fondem, případně s centrálními bankami.
- Komunikace mezinárodních jednotek nasazených v místě humanitární krize. Zde se jedná zejména o zahraniční vojenskou, záchranářskou nebo zdravotnickou účast, která potřebuje komunikovat se svými národními nadřízenými stupni.

Dále je zde na tomto místě vhodné zmínit i jiné relevantní subjekty, které potřebují komunikovat v průběhu krizové události:

- Komunikace příslušníků mezinárodních nevládních organizací s jejich mateřskými kancelářemi. Komunikace jednotlivých občanů s rodinnými příslušníky pobývajícími v zahraničí. Komunikace zaměstnanců zahraničních soukromých společností s mateřskou centrálou.
- Přímá komunikace turistů pobývajících v postižené zemi s domovem. Tuto lze v nutném případě zajistit prostřednictvím národního velvyslanectví nebo ambasády.
- Komunikace soukromých firem se zahraničními dodavateli nebo odběrateli.

Komunikace národní

Tato infrastruktura zajišťuje komunikaci v širokém spektru uživatelů. Opět zde máme hlasovou a datovou komunikaci, popř. videokonferenční jednání, které můžeme rozdělit na **utajované** a **neutajované**:

- Oficiální komunikace na úrovní vlády a ministerstev, která zabezpečuje chod státu i v době krize. V úvodu krize je důležitá zejména komunikace v rámci ministerstev vnitra, obrany a zdravotnictví. V pozdějších fázích vstupují do popředí ministerstva mající v popisu místní rozvoj nebo sociální aspekty obyvatel.
- Komunikace ministerstev s jejich podřízenými složkami a útvary.
- Komunikace v rámci jednotlivých ozbrojených složek.
- Komunikaci mezi jednotlivými zdravotnickými a farmaceutickými institucemi.

Další subjekty, které mohou využívat vnitrostátní popř. národní komunikaci:

- Vzájemná komunikace příslušníků mezinárodních nevládních organizací.
- Komunikace jednotlivých občanů s rodinnými příslušníky.
- Komunikace soukromých společností nepodílejících se na vypořádání s krizí případně s jejími následky.

Komunikace oblastní

Tato infrastruktura zajišťuje komunikaci mezi jednotkami zainteresovanými přímo centru humanitární krize. Nejdůležitějšími body této komunikace jsou jednotlivé

krizové štáby, místní centrály státní a městské policie, místní a oblastní hasičské stanice a v neposlední řadě také nemocnice a další zdravotnická zařízení. Tato úroveň požaduje časově neomezenou hlasovou a datovou komunikaci. V případě hlasové komunikace vyvstává také požadavek na mobilní komunikaci, zajišťovanou zejména ručními radiostanicemi s mobilním pokrytím signálu.

3.1 Integrovaná Komunikační Síť Ministerstva Vnitra

Ke krizové komunikaci slouží účelová síť ministerstva vnitra, která zabezpečuje hlasovou a datovou komunikaci a připojení hromadné radiokomunikační sítě integrovaného záchranného systému a zajišťuje kompletní telekomunikační služby mezi všemi subjekty MV, Policie ČR, HZS ČR a všech ostatních složek integrovaného záchranného systému. Jednotlivé komunikační služby ITS MV jsou:

- hlasové služby – systém HELIOS, propojení jednotlivých komunikačních uzlů pro hlasové komunikace,
- radiové služby – systém PEGAS, propojení technologií digitální radiové sítě PEGAS (radiové ústředny, mainswitche, BS – základnové radiové stanice),
- datové služby – systém HERMES, provoz intranetu, elektronické pošty, GINIS a podobně,
- dohledová síť – viz také [20].

3.1.1 Operační a informační střediska IZS

Operační a informační střediska IZS jsou stálými orgány pro koordinaci složek IZS. Podle §5 zákona o IZS plní úkoly operačních a informačních středisek IZS operační a informační střediska HZS krajů a operační a informační středisko MV – generálního ředitelství HZS ČR. Zřizování operačních a informačních středisek HZS ČR se řídí zvláštním právním předpisem. Vedle úkolů na úseku požární ochrany a IZS plní operační a informační střediska IZS také úkoly vyplývající z dalších právních předpisů, např. zákona o vodách, atomového zákona a zákona o prevenci závažných havárií. Operační a informační střediska IZS jsou povinna:

- přijímat a vyhodnocovat informace o mimořádných událostech, za tím účelem obsluhují také tísňovou linku 150 a 112, jejímž prostřednictvím může každý iniciovat systém IZS k zásahu v případě mimořádné události,

- zprostředkovávat plnění úkolů ukládaných velitelem zásahu zejména jeho žádosti o potřebné síly a prostředky,
- vyhlášení odpovídajícího stupně poplachu pro místo zásahu,
- poskytnutí osobní nebo věcné pomoci potřebné pro záchranné a likvidační práce.
- plnit úkoly uložené orgány oprávněnými koordinovat záchranné a likvidační práce,
- zabezpečovat v případě potřeby vyrozumění základních i ostatních složek integrovaného záchranného systému a vyrozumění státních orgánů a orgánů územních samosprávných celků podle IZS [21].

Operační a informační střediska IZS jsou také oprávněna:

- povolávat a nasazovat síly a prostředky hasičského záchranného sboru a jednotek požární ochrany, dalších složek IZS podle poplachového plánu IZS, nebo podle požadavků velitele zásahu,
- provést při nebezpečí z prodlení varování obyvatelstva na ohroženém území.

Základním úkolem operačních a informačních středisek IZS je také zajistit nepřetržitou podporu činnosti krizovým štábům a výměnu informací z míst mimořádných událostí do krizového štábu a mezi krizovými štáby a to i v případech, kdy spolehlivě nefungují veřejné komunikační prostředky, je nefunkční elektrická rozvodná síť a podobně [21].
Operační středisko IZS rovněž:

- dokumentuje záchranné a likvidační práce, na kterých se podílí,
- spolupracuje na zpracování dokumentace IZS,
- udržuje spojení s operačními středisky základních složek IZS a s ostatními složkami, s místy zásahu a s krizovými štáby,
- vyhlašuje odpovídající stupeň poplachu při prvotním povolávání a nasazování sil a prostředků,
- vyhlašuje odpovídající stupeň poplachu pro území postižené mimořádnou událostí, jestliže je na tomto území více jak jedno místo zásahu,
- předává informaci o vyhlášeném třetím nebo zvláštním stupni poplachu pro území postižené mimořádnou událostí organizačně vyššímu operačnímu a informačnímu středisku,

- zapojuje se do mezinárodních záchranných operací a do příhraniční spolupráce při záchranných a likvidačních pracích podle zákona o IZS.

Obsahem předávaných informací cestou operačních a informačních středisek IZS na kraje (krizové štáby krajů) nebo obce (krizové štáby určených obcí) jsou zejména:

- upozornění a výstrahy na možný výskyt závažných mimořádných událostí,
- informace o vzniku a vývoji závažných mimořádných událostí,
- informace o vyhlášení ústřední koordinace záchranných a likvidačních prací,
- informace o spuštění varovacího systému, včetně doplňkových informací,
- informace o vyhlášení krizových stavů včetně informací o činnosti krizových orgánů,
- nabídky pomoci z vyšší úrovně,
- požadavky na informace pro vyšší úroveň [21].

Obsahem předávaných informací z kraje (krizové štáby krajů) nebo obce (krizové štáby určených obcí) cestou OPIS IZS na vyšší úroveň jsou zejména:

- situační zprávy,
- požadavky na zajištění pomoci,
- informace vyžádané z vyšší úrovně.

Operační středisko základní složky může, pokud je to technicky možné přepojit tísňové volání přímo na základní složku, která je k řešení mimořádné události příslušná, nebo na operační středisko územně příslušné základní složky, nebo na územně příslušné operační a informační středisko IZS. Na obdobném principu pracuje obsluha tísňové linky 112. Základní složky IZS jsou informovány o nebezpečích vzniku mimořádných událostí prostřednictvím operačních a informačních středisek IZS. Je-li to nutné pro provádění záchranných a likvidačních prací, operační a informační střediska IZS o nebezpečích vzniku mimořádných událostí určené osoby dotčených správních úřadů s působností na území kraje nebo obcí a určené právnické a fyzické osoby havarijním plánem kraje [21]. Komunikační a informační technologie ve složkách IZS jsou podrobně rozepsány v příloze č. 5.

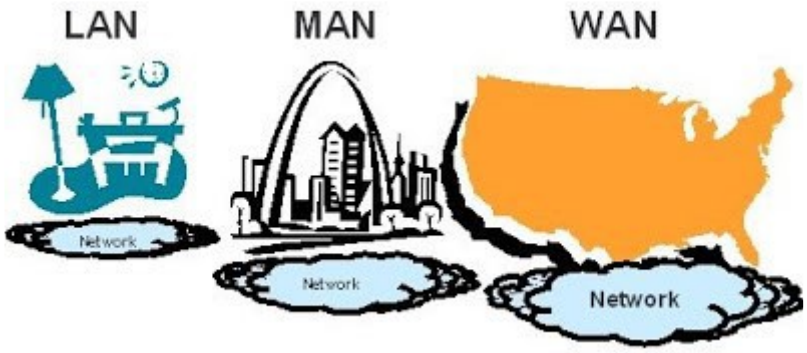
3.2 Počítačové sítě

Pojmem počítačová síť je označen souhrn technických prostředků, které realizují propojení mezi koncovými zařízeními a jejich vzájemnou komunikaci za určitých předem definovaných pravidel. Počátky vzniku sítí sahají až do 60. let minulého století, kdy začali první pokusy s propojováním počítačů. V dnešní době jsou sítě pospojovány do globální sítě – internet.

Počítačové sítě mají různé druhy dělení. Dělení podle druhu přepojování, podle druhu přenášeného signálu, podle přenosu dat, podle uživatele – viz také [22], [23], [24]. Nejčastěji se však setkáme s dělením z hlediska velikosti sítě – viz obr. 3.1. Počítačové sítě jsou zde děleny do 4 základních skupin:

- PAN (Personal Area Network) - tzv. osobní síť je malá síť, která propojuje osobní elektronická zařízení typu tablet, mobilní telefon či notebook.
- LAN (Local Area Network) - tzv. místní síť je síť na úrovni budovy či několika blízkých budov do maximální vzdálenosti několik kilometrů. Typická je například podniková síť.
- MAN (Metropolitan Area Network) - tzv. metropolitní síť je síť propojující lokální sítě v městské zástavbě.
- WAN (Wide Area Network) - tzv. rozlehlá síť, která propojuje jednotlivé menší sítě v jeden celek.

Obr. 3.1 Dělení počítačových sítí dle velikosti



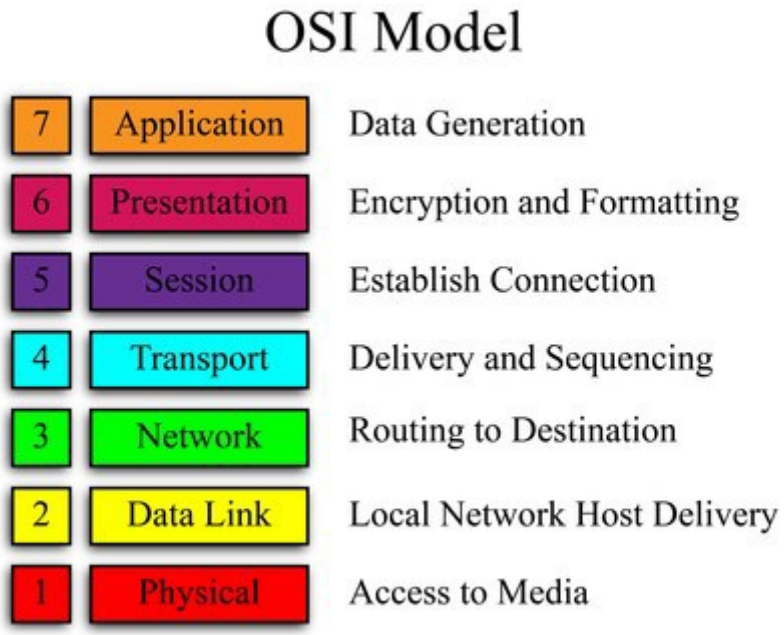
Zdroj:[27]

3.2.1 Model ISO/OSI

Tento model vypracovala organizace ISO jako část snahy o standardizaci počítačových sítí. V roce 1984 byl přijat jako mezinárodní norma ISO 7489. Tento model používá názorný příklad komunikace v počítačových sítích pomocí vrstveného modelu, kde jsou vrstvy nezávislé a nahraditelné.

Norma nespecifikuje žádné implementace, ale uvádí princip síťové architektury za pomocí sedmi vrstev – viz obr. 3.2. Popisuje jejich funkce a služby, avšak nezavádí žádné protokoly, které by vyžadovaly příliš mnoho detailů [25], [26].

Obr. 3.2 Referenční OSI Model



Zdroj: [27]

3.2.2 Pasivní prvky sítí LAN

Pasivní síťové prvky (anglicky Passive Networking Components nebo Passive Networking Hardware) jsou ty části počítačové sítě, které fyzicky zajišťují přenos dat v síti. Zjednodušeně lze říci, že je to především kabeláž a všechny nutné prvky kolem (zásuvky, spojky a podobně).

Co patří mezi pasivní síťové prvky:

- Kabely (optické kabely, koaxiální kabely, kroucená 4 linka),
- Konektory,
- Rozvaděče,
- Spojky,
- Zásuvky.

Na rozdíl od aktivních síťových prvků nespotřebovávají pro svůj provoz žádnou elektrickou energii a také žádným způsobem nemění ani neovlivňují data, která přes ně proudí. Souhrnně můžeme pasivní část sítě nazvat strukturovanou kabeláží.
Strukturovaná kabeláž je pasivní částí fyzické vrstvy. Jde o kabelážní systémy pro přenos dat, hlasu a dalších služeb v rámci integrovaného provozu budov. Používají se datové kabely se čtyřmi kroucenými páry a optický kabel. Hlavní výhoda strukturované kabeláže je:

- univerzálnost,
- modularita,
- flexibilita [25].

Pravidla pro návrh a instalaci strukturované kabeláže jsou od počátku 90. let normalizovány různými standardizačními organizacemi. Důvodem je nutnost vytvořit jednotná pravidla pro datové, telekomunikační a jiné kabelážní systémy budov. Tyto normy stanovují postup správné instalace, její rozšiřování a případné změny. Samotné normy vytvářejí a schvalují komise pro dané oblasti. Komise jsou složeny z výrobců, univerzit, konzultantů a států. Důvodem této snahy o sjednocení a harmonizaci pomocí norem je poskytnout zajímavé produkty a služby koncovým zákazníkům a umožnit detailně specifikovat požadovaný produkt, aniž by bylo nutné zacházet do technických podrobností.
Mezi celosvětovými a americkými standardy jsou některé méně či více závažné rozdíly. Za jeden z nejdůležitějších se dá považovat skutečnost, že dokumenty ISO/IEC definují tzv. třídy vedení (např. Class D nebo Class E) a jejich vlastnosti, které má strukturovaná kabeláž splňovat jako celek. Oproti tomu ANSI / EIA / TIA normy deklarují požadované vlastnosti spíše pro jednotlivé komponenty v rámci tzv. kategorií (např. kategorie 5e nebo kategorie 6).

V Evropské unii jsou ISO normy přebírány organizací Cenelec a jako ČSN EN normy platí v České republice [27].

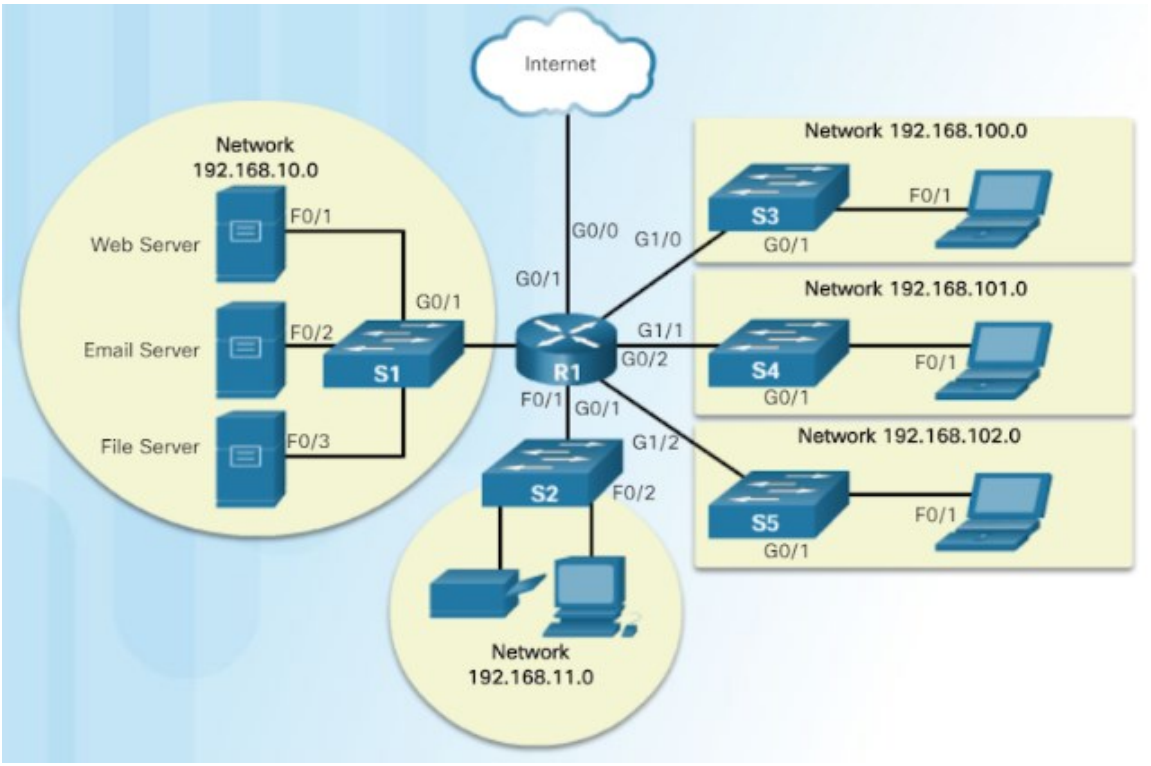
3.2.3 Aktivní prvky sítí LAN

Aktivní síťové prvky jsou ty části počítačové sítě, které nějakým způsobem aktivně pracují se signály v síti (zesilují je, modifikují, vyhodnocují atd.). Aktivní síťové prvky jsou zpravidla konkrétní zařízení umístěná v uzlech sítě.
Mezi aktivní síťové prvky se řadí:

- Switch (Přepínač),
- Repeater (Opakovač),
- Hub (Rozbočovač),
- Bridge (Můstek),
- Router (Směrovač),
- Tiskový server (Print Server),
- Access point (AP), přístupový bod,
- Firewall.

Aktivní síťové prvky jsou nezbytnou součástí každé počítačové sítě. Řídí tok dat nebo signálu v síti, například jej zesilují, propojují, modifikují, přesměrovávají, a starají se také o bezpečnost. Nejsou tedy jen mechanickou součástí, ale jedná se vlastně o počítače, nebo alespoň o aktivní čipy, na kterých běží nějaký software, který něco řídí. Proto jsou aktivní, a proto i výkonnost aktivních prvků záleží nejen na kvalitě a výkonnosti jejich čipů, ale zejména na kvalitě řídícího software.
Obrázek 3.3 znázorňuje použití síťových zařízení a koncových prvků v logické topologii sítě.

Obr. 3.3 Logická topologie sítě



Zdroj:[30]

Mezi aktivními prvky jsou chytřejší (pracující na vyšších úrovních) a hloupější zařízení. Například opakovače nebo jednoduché přepínače (switche) se signálem nijak dál nepracují, nechápou ho (nerozlišují například škodlivý software od normálního), pouze se starají o jeho přenos dál. Na druhou stranu routery, firewally, nebo bridge už pracují s daty na vyšší úrovni a dokážou odfiltrovat kybernetické útoky [27].

Opakovač

Opakovač (anglicky repeater) je elektronický aktivní síťový prvek, který přijímá zkreslený, zašuměný nebo jinak poškozený signál a opravený, zesílený a správně časovaný ho vysílá dále. Tak je možné snadno zvýšit dosah média bez ztráty kvality a obsahu signálu.

Opakovače patří do první (fyzické) vrstvy referenčního modelu OSI, protože pracují přímo s elektrickým signálem. Více opakovačů za sebou umožňuje prodloužit dosah signálu.

U Ethernetu je z důvodu použití kolizních protokolů CSMA/CD jejich počet omezen, aby bylo možné bezpečně detekovat kolize. Použití opakovačů totiž vnáší

nezanedbatelné zpoždění do celkové doby, kterou signálu trvá, než urazí cestu z jednoho konce sítě na druhý. Pokud by tato doba přesáhla určitou hranici, mohlo by dojít k nežádoucí situaci: kolize by byla detekovatelná jen v části sítě, a nikoli v celé síti (například jen "uprostřed", a nikoli "na koncích").

Rozbočovač

Rozbočovač (anglicky Hub) je velmi jednoduché aktivní síťové zařízení. Nijak neřídí provoz, který skrz něj prochází a pracuje na fyzické vrstvě (1. vrstva) modelu OSI. Signál, který do něj vstoupí, je obnoven a vyslán všemi ostatními porty. Zpoždění je proto pouze 1 bit, takže na rozdíl od síťového přepínače způsobuje hub nižší latenci. K tomu aby byly síťové prvky schopny detekovat kolize, je počet rozbočovačů v síti omezen. Pro síť 10 Mbit/s je počet segmentů omezen na 5 (4 rozbočovače) mezi dvěma koncovými stanicemi. U sítě 100 Mbit/s je limit snížen na 3 segmenty (2 rozbočovače). Některé huby mají speciální port, který umožňuje jejich slučování, takže se navenek chovají jako jeden (anglicky stack) [27].

Síťový přepínač

Síťový přepínač (anglicky switch) je v informatice aktivní prvek v počítačové síti, který propojuje jednotlivé prvky do hvězdicové topologie. Přepínač obsahuje větší či menší množství síťových portů (až několik stovek), na něž se připojují síťová zařízení nebo části sítě. Přepínač přeposílá síťový provoz jenom do těch směrů, do kterých je to potřeba, čímž se odlišuje od jednoduššího hubu.

S přepínačem se nejčastěji setkáváme jako s aktivním prvkem v síti Ethernet realizované kroucenou dvojlinkou. Zde nahradil dříve používané huby (rozbočovače), které signál jednoduše kopírovaly do všech ostatních rozhraní. Pracuje zde na 2. vrstvě OSI modelu. Vedle vyššího výkonu (stanice připojené k různým rozhraním přepínače navzájem nesoutěží o médium) znamená přínos i pro bezpečnost sítě, protože médium již není sdíleno a data se vysílají jen do rozhraní, jímž je připojen jejich adresát.

Adresování se přepínači učí automaticky z procházejícího provozu, konkrétně z adres odesilatelů uvedených v rámcích, které do přepínače přicházejí. Používá se algoritmus Backward Learning Algorithm. Z těchto údajů si přepínač automaticky plní tabulku identifikující cílová rozhraní pro jednotlivé adresy. Pokud přepínač dostane k doručení rámec směřující na jemu dosud neznámou adresu, chová se jako hub a rozešle rámec do

všech ostatních rozhraní. Lze očekávat, že oslovená stanice pravděpodobně odpoví a přepínač se tak vzápětí dozví, kde se nachází.

Ethernetové přepínače mají problém se smyčkami v síti, vytvářenými za účelem redundance. Pokud síť obsahuje smyčku (mezi dvěma uzly existuje více než jedna cesta), mohou pakety od stejného odesilatele přicházet chaoticky z různých rozhraní a dokonce tentýž paket může do přepínače dorazit několikrát. Přepínač není v takovém prostředí schopen rozpoznat, kde se kdo nachází. Tento problém řeší přepínače mechanismem zvaným Spanning Tree Protocol, kterým se dohodnou na nepoužívání některých tras tak, aby ze sítě zmizely smyčky. Vytvoří se minimální kostra sítě dosahující do všech jejích míst. Když dojde ke změně v topologii (např. rozpojení některé linky), bude aktivována některá z dosud odstavených tras tak, aby nový strom nadále pokud možno pokrýval celou síť. Tyto změny se ovšem nedějí okamžitě, je zde jisté zpoždění [27].

Přepínače dnes často nabízejí i některé pokročilejší funkce, jako například:

- Management – možnost upravovat nastavení přepínače pomocí telnetu nebo webového rozhraní (HTTP),
- VLAN – podpora virtuálních sítí,
- SNMP – vzdálená správa zařízení, hlášení určitých stavů a situací apod.,
- Shortest Path Bridging – se záměrem zjednodušit vytváření a konfigurování sítí s možností vícecestného směrování.

Kromě klasických přepínačů (tzv. layer 2), které pracují na linkové vrstvě, existují i pokročilejší přepínače, které rozhodují o cíli přijatého rámce na základě informací z vyšších síťových vrstev a složitějších pravidel. Pokud je rozhodnutí založena na IP adrese, označují se takové přepínače jako layer 3. Je-li rozhodnutí prováděno nejen podle IP adresy, ale i podle čísla síťového portu, označují se jako layer 4. Číslo zde označuje pořadí síťové vrstvy v referenčním modelu ISO/OSI [27].

Směrovač

Pro komunikaci v počítačových sítích je třeba krom použitých protokolů zajistit doručení na určené místo nejvhodnější cestou. K tomuto účelu se využívá zařízení zvané směrovač (router) a vhodný routovací mechanizmus. Směrovač (router) je v počítačových sítích aktivní síťové zařízení, které procesem zvaným routování

přeposílá datagramy směrem k jejich cíli. Routování probíhá na třetí vrstvě referenčního modelu ISO/OSI (síťová vrstva).

Netechnicky řečeno, router spojuje dvě sítě a přenáší mezi nimi data. Router se podstatně liší od switche, který spojuje počítače v místní síti. Rozdílné funkce routerů a switchů si lze představit jako switche coby silnice spojující všechna města ve státě a routery coby hraniční přechody spojující různé země. Routování je většinou spojováno s protokolem IP, ačkoliv se stále používají i jiné, méně populární protokoly.

Router používá routovací tabulku, která obsahuje nejlepší cesty k jistým cílům a routovací metriky spojené s těmito cestami. Viz routování. Nedávno se routovací funkce začaly přidávat ke switchům, čímž vznikly switche „Layer 2/3“, které routují provoz rychlostí srovnatelnou s rychlostí linky.

Routery se nyní implementují také jako „internetové brány“, primárně pro malé sítě jako ty používané doma a v malých kancelářích. Používají se hlavě tam, kde je internetové připojení rychlé a „vždy připojené“, jako kabelový modem nebo DSL. Tato zařízení ale nejsou v principu routery, protože počítače ve vnitřní síti efektivně skrývají pod svoji vlastní IP adresu ve vnější síti. Tato technika se nazývá NAT (network address translation, překlad adres).

Pro malé sítě je asi nejvhodnější statický routing, kdy se manuálně zadají směry do routovací tabulky. Pro větší sítě je již vhodné použít typ dynamického routingu pomocí routovacího protokolu. Máme dva základní typy routovacích protokolů: Link-State a Distance Vector. Pro opravdu velké sítě typu MAN/WAN se používá Path Vector Protocol a jeho zástupce BGP (Border Gateway Protocol) [28], [29].

3.2.4 Design sítí

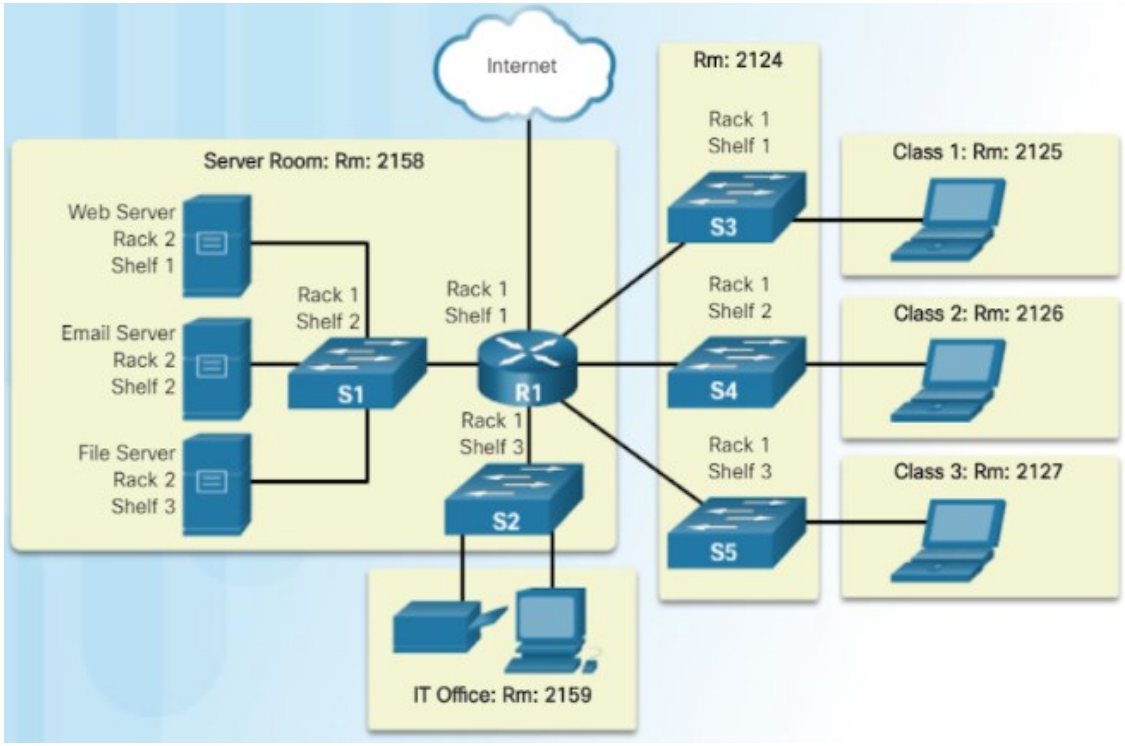
Při návrhu sítí je třeba dbát na základní pravidla vycházející z doporučení předních výrobců a doporučení vycházející z dlouhodobé zkušenosti z praxe. Je dobré mít na paměti základní pravidla, které platí v plánování lokálních sítí:

- Správně definovat cíl – je třeba vědět, pro co se bude síť používat a dle toho navrhnout design, mít možnost síť rozšiřovat bez zásadní změny designu a výpadků a zajistit konvergenci sítě.
- Bezpečnost – přemýšlet již v návrhu nad možnostmi zabezpečení dat v síti před vnějším i vnitřním nebezpečím (Firewall, VLAN, access listy).

- Zálohování – souvisí z bezpečností. Obnova musí být co nejméně náročná, ať se dají minimalizovat ztráty způsobené výpadky. Dobře rozmyslet redundanci centrálních prvků, řešení pomoci clusteringu serverů apod.
- Monitoring – navrhnout vhodné řešení monitoringu zařízení v síti, která bude v pravidelných intervalech hlídat kritické prvky sítě, a bude včas informovat o výpadku. Dále možnosti sledování toku dat v síti, pomocí vhodné sondy.
- Centrální správa – mít možnost spravovat systémy v síti pomoci jedná aplikace pro danou technologii.

Pro názornost je na obrázku č. 3.4 znázorněná možná konfigurace fyzické topologie síťových a koncových zařízení.

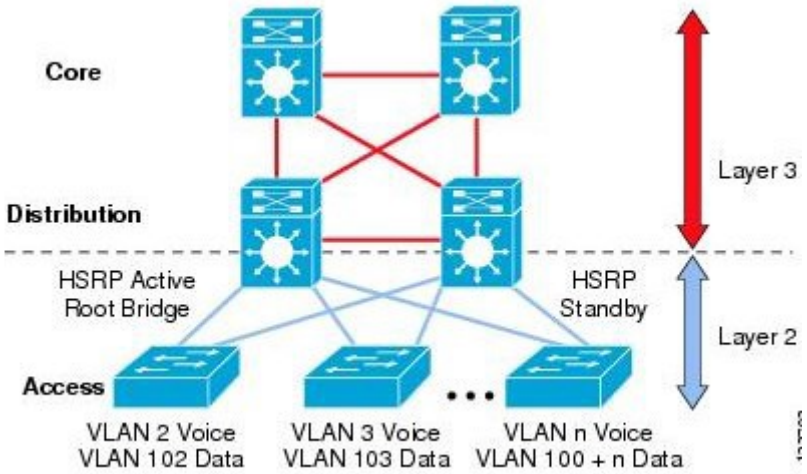
Obr. 3.4 Fyzická topologie sítě



Zdroj: [30]

Pro sítě typu LAN, je dobré použít hierarchický, tří úrovňový design, s L3 distribucí – viz obr. 3.5 [27].

Obr. 3.5 Tří úrovňový design s L3 distribucí



Zdroj: [27]

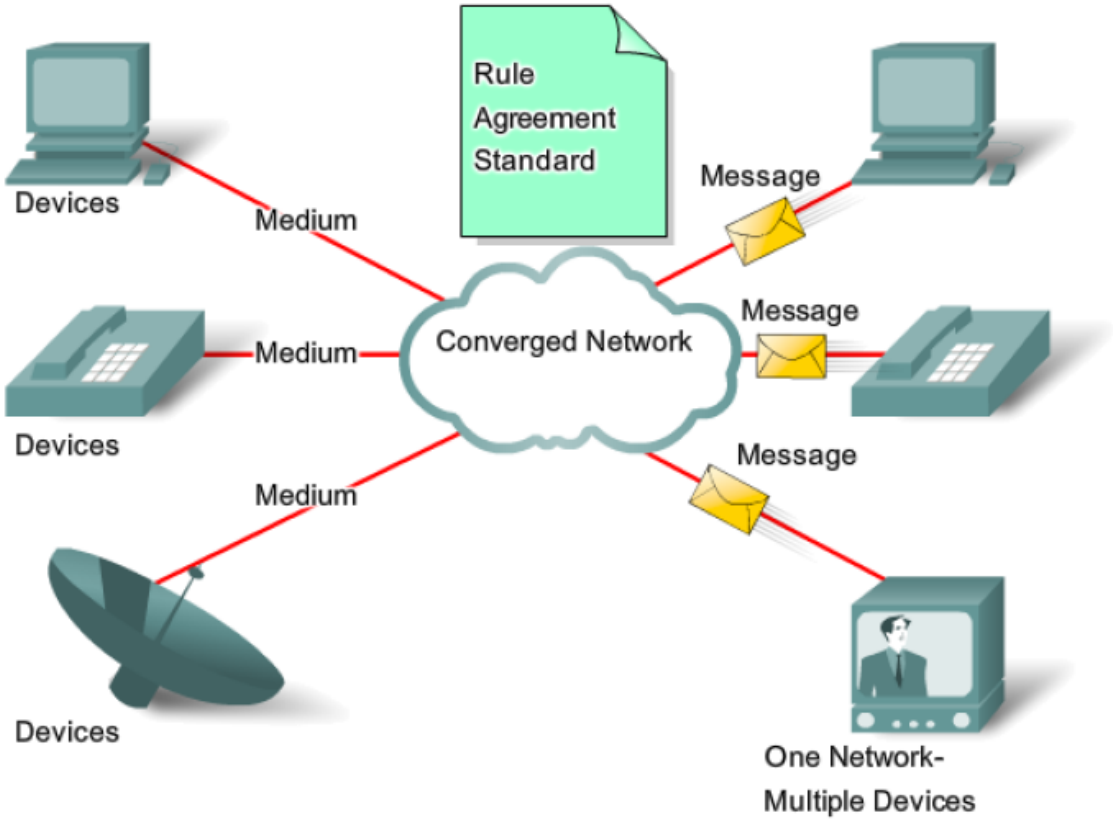
3.2.5 Konvergované a dedikované sítě

Struktury vyhrazených (dedikovaných) sítí pouze pro jedinou službu jsou již z dnešního pohledu zastaralé. Tyto struktury se někdy také nazývají paralelní, neboť služby jako telefonie, televizní vysílaní nebo datové služby jsou poskytovány paralelně – nezávisle jedna na druhé (jak technologicky – samostatná, nesdílená vedení, tak aplikačně – vzájemně nesourodá softwarová řešení).

Ukazuje se, že udržování infrastruktury vhodné pouze pro hlasové přenosy (telefonie) a budování přenosových cest pro šíření datových sítí (internet), je velice nákladné. Významných úspor lze docílit zavedením konvergovaných sítí:

Konvergovaná síť je taková, ve které existuje jedna platforma pro všechny služby. Prostřednictvím ní lze poskytovat telefonii, televizní streaming i internetové služby. Příkladem konvergence služeb je portfolio služeb nabízené společností Telefonica O2.

Obr. 3.6 Představa konvergované datové sítě



Zdroj: [31]

4 NÁVRH INTEGRACE KOMUNIKAČNÍCH SLUŽEB DO POST-KRIZOVÝCH LOGISTICKÝCH PROCESŮ

Klíčovým prvkem organizace pomoci je komunikace v reálném čase. V rámci post-krizových logistických procesů bude vyžadována zejména hlasová a datová komunikace. Na vyšší úrovni potom také komunikace audiovizuální. Při zasazování komunikačního uzlu do procesu odstraňování následků krize jsem počítal s jednotlivými centry, která musí být komunikačně obsluhována.
Již ve fázi nácviků a plánování pro zasazení komunikačních center do post-krizových logistických procesů musí být zřejmé všechny varianty struktury komunikačního a informačního datového toku tak, aby potřebné centrum mohlo být vystavěno v korektním časovém limitu a stalo se tak operační.

Obsluhovaná centra

- Počet obsluhovaných **center národní úrovně** – do této úrovně počítám celostátní krizový štáb, některé další organizace státní správy.
- Počet obsluhovaných **center oblastní úrovně** – na této úrovni se jedná zejména o krajský krizový štáb, případně krizový štáb obce.
- Počet obsluhovaných **center lokální úrovně** – Na lokální úrovni budou obsluhovaná centra zajišťovat komunikační služby zejména národním a mezinárodním jednotkám humanitární pomoci, národním a mezinárodním humanitárním organizacím vyslaným do míst postižených krizí a dalším objektům a organizacím podílejícím se na odstraňování následků krizí.

4.1 Návrh konkrétního komunikačního centra

Navrhované informační centrum pro účely této diplomové práce jsem vystavěl výhradně na operačních systémech a službách společnosti Microsoft.
Svůj návrh zaměřuji na základní služby funkčních aplikací komunikačních a informačních systémů, které pomohou v prostoru nasazení plnit úkoly vyplývající z krizové situace. Nad rámec lze však použít software, který se specifikuje přímo na danou oblast komunikace (např. navádění vzdušných prostředků, aplikační vybavení pro zdravotnickou pomoc, atd.) a zefektivnit ještě více nasazení komunikačního centra.

Následuje popis jednotlivých sekcí s přiloženými schématy návrhu.

4.1.1 Sekce obsluhy serverů, informační služby, coreservices

Všechny úrovně operačního centra potřebují pro přenos datového toku výkonné servery, které slouží jako hlavní pilíře pro základní služby jádra komunikačního centra, tzv. *coreservices.* Pro využití jakékoliv varianty krizového scénáře je nutno mít dostačující konfiguraci fyzických serverů, respektive komponentů, které servery obsahují. Proto zdůrazňuji nutnost brát zřetel na výkon procesoru, velikost RAM, kapacitu a rychlost HDD, síťové karty, atd.

Fyzické servery navrhuji rozdělit na virtuální pomocí dostupného softwarového vybavení, jako např. VMware nebo Microsoft Hyper-V.

Níže popíšu jednotlivé služby, které navrhuji implementovat do komunikačního centra na všech úrovních.

DC – Domain Controller – Doménový Řadič

V každé soustavě serverů, potažmo v navrhovaných komunikačních centrech všech úrovní musí být vždy alespoň jeden doménový řadič, který zpravidla bývá určen jako fyzický server, na kterém běží nezbytné služby jádra (*coreservices*). Primární doménový řadič označujeme jako PDC (primary domain controller) a záložní doménový řadič bývá označován jako BDC (backup domain controller). Pro funkci Doménového Řadiče vyberu stabilní výkonný server, který vytvoří hlavní páteřní pilíř pro služby, které budou v případě mnou navrhovaného komunikačního centra využívány. Na DC budou instalovány a konfigurovány služby, jako např. DNS *(Domain Name Server)*, *Active Directory*, NTP Server *(Network Time Protocol Server)* a jiné. Tyto tři výše uvedené služby v následující podkapitole stručně popíšu spolu se schématy návrhu implementace jednotlivých služeb do DC serverové soustavy navrhovaného komunikačního centra.

DNS (Domain Name Server)

Jedná se o službu, která určuje hierarchický systém doménových jmen a která je realizovaná serverem DNS, v tomto případě pak fyzickým serverem DC. Služba DNS využívá stejnojmenný protokol pro výměnu informací o překladech doménových jmen a transferových uzlů na srozumitelný uživatelský název např. webového rozhraní.

Schéma návrhu implementace služby DNS je uvedeno na obrázku 4.1.

Active Directory

Active Directory je služba společnosti Microsoft, která funguje na bázi protokolu LDAP *(Lightweight Directory Access Protocol)*, který je definovaný pro ukládání a přístup k datům na adresářovém serveru, v mém případě na doménovém řadiči. *Active Directory* bude v tomto případě adresářová služba, která bude sloužit pro ukládání individuálních uživatelských účtů se všemi informacemi o uživatelích, popř. uživatelských skupin (pro zvláštní přístup do vyčleněných adresářů, apod.). Hlavní cíl služby bude v našem případě ověřovat uživatele, skupiny, počítače a jiné zařízení vůči doménám, a dále spravovat bezpečnostní politiky nastavení systému komunikačního centra.

Schéma návrhu implementace služby *Active Directory* je uvedeno na obrázku 4.2.

NTP – Synchronizace času

Služba NTP je nedílnou součástí každé domény. Funguje na bázi stejnojmenného protokolu – *Network Time Protocol*, který zajišťuje, aby všechna zařízení v síti (především ostatní fyzické i virtuální servery a pracovní stanice) měla stejný a přesný čas. Byl navržen tak, aby odolával následkům proměnlivých zpoždění v doručování paketů.

Schéma návrhu implementace služby serveru NTP je znázorněno na obrázku 4.3.

Další služby, které jsou důležité pro korektní zabezpečení chodu navrhovaného komunikačního centra, budou instalovány na virtuální servery, které budou dynamicky fungovat na fyzických serverech VH *(Virtual Hosts).*

Antivirový systém – EndPoint Security

Velmi důležitou službou, která bude monitorovat veškerou činnost na doménách komunikačního centra je Antivirový systém. Služba poběží nepřetržitě na zvláštním virtuálním serveru a její databáze se bude zálohovat na jiném vyčleněném SQL serveru. Antivirový systém komunikačního centra neslouží pouze pro detekci hrozby v podobě virů, malware, Spyware, Trojans, apod., ale také pro monitorování přihlašování uživatelských účtů, vkládání veškerých HID zařízení do portů USB, aktualizace virových databází koncových zařízení, monitorování korektních klasifikací utajení dokumentů a jiné možnosti monitorování bezpečnosti domény.

Pro návrh komunikačního centra jsem jako hlavní antivirový systém zvolil produkt společnosti McAfee – ePolicy Orchestrator.

Schéma implementace antivirového systému pro komunikační centrum uvádím na obrázku 4.4.

WSUS – Aktualizace operačních systémů

WSUS*(Windows Server Update Services)* je služba společnosti Microsoft, která v návrhu komunikačního centra poběží na zvláštním virtuálním serveru a bude monitorovat a odesílat potřebné aktualizace jak na ostatní servery, tak na koncové stanice. Administrátor této služby může přes její prostředí dohlížet na spravované zařízení a také částečně regulovat aktualizace stanic. Toto je možné především z důvodů jednorázového zahlcování sítě velkým tokem dat a možnosti neodeslání aktualizace, která není odladěná a vytváří problémy koncovým uživatelům.

Pokročilou správu aktualizací společnosti Microsoft pak nabízí produkt rodiny *System Center – SCCM (System Center Configuration Manager).* Jelikož se však jedná o velmi pokročilou hloubkovou správu systému, Produkty *System Center* rodiny nejsou předmětem návrhu komunikačního centra.

Aktualizace společnosti Microsoft se nahrávají automaticky po připojení WSUS serveru k internetu. Na utajených doménách lze službu nastavit pro ruční vkládání stažených aktualizací a následné odesílání na spravované zařízení ze serveru. V mém případě návrhu komunikačního centra projde aktualizace nejdříve antivirovou kontrolou, dále testovacím prostředím a ověření funkčnosti bude nahrána na WSUS server.

V případě nasazení jiných, operačních systémů, např. na bázi UNIX je ve většině případů systém instalován ve virtualizačním prostředí HyperV nebo VMware a používán pro běh softwarových nástrojů určených k bezpečnostní kontrole počítačové sítě (nástroje NESSUS, LAN SWEEPER). Této možnosti se využívá především pro velmi nízké hardwarové nároky, které dovolí skenování sítě i při jejím běžném provozu. V případě pracovních stanic je tento operační systém používán výhradně na počítačích se statusem „Stand Alone“ (trvale nepřipojených do sítě). Tyto počítače jsou buď vybaveny softwarovými nástroji určenými k digitálnímu forenznímu vyšetřování, nebo naopak hackovacím programovým vybavením určeným k preventivnímu penetračnímu testování bezpečnostního zabezpečení sítě.

Schéma služby WSUS je znázorněno na obrázku 4.5.

Chat – komunikace pomocí krátkých rychlých zpráv

Chat mezi uživateli a ve skupině uživatelů je dalším důležitým pomocníkem pro navrhované komunikační centrum. Jedná se o službu ze skupiny FAS *(Functional Area*

Services), která je určena jako podpora uživatele pro plnění dílčích úkolů v krizové situaci. Aplikací, které nabízejí softwarový chat, je široká škála. Pro uvedené komunikační centrum jsem zvolil aplikaci J-Chat, která je otestovaná a nasaditelná i pro utajovanou doménu.

Schéma aplikace J-Chat v navrhovaném komunikačním centru je znázorněno na obrázku 4.6.

SharePoint – webový komunikační portál

Jako další důležitý komunikační prvek v krizovém centru navrhuji komunikační webový portál, který je určen především pro informace o aktuálním dění krizového scénáře, sdílení úkolů, poznatků, zpravodajství, atd. SharePoint bude také v mnou navrhovaném případě sloužit jako sdílené datové úložiště pro registrované uživatele. V případě potřeby sdílet klasifikované informace doporučuji portál vytvořit také na utajované doméně.

Schéma SharePointu je znázorněno na obrázku 4.7.

Poštovní server – Mail Exchange

Zřejmě nejdůležitější a nejžádanější službou v komunikačním centru je poštovní komunikace. Poštovní server navrhuji implementovat odděleně od ostatních a doporučuji nastavit u něj lepší konfiguraci pro možnost zvýšeného datového toku. Důležité je také propojení na databázový server SQL pro ukládání dat jako např.: jméno, příjmení, organizace, mailová adresa, doména, atd. Důležitá je také konfigurace serveru pro korektní funkčnost aplikace Microsoft Outlook, popř. OWA (Outlook Web Access), který bude součástí navrhovaného komunikačního centra.

Schéma návrhu poštovního serveru je znázorněno na obrázku 4.8.

4.1.2 Sekce satelitního přenosu

Jedním z komunikačních přenosových prostředí navrhuji použití satelitního širokospektrálního přenosu do místa krizové události – viz teoretická část práce. Satelitní pásmo je globálně dostupné prakticky na 99% území naší planety. Díky velmi hustému pokrytí různými družicemi v různých pásmech lze získat potřebná data se zpožděním max. v řádu vteřin kdekoliv na světě. Při použití satelitní technologie je potřeba kromě terminálového zabezpečení mít vyřešeno správně objednané satelitní pásmo a jasně dohodnuté podmínky využití. Nejvíce využívaná frekvenční pásma pro satelitní přenos dat jsou v dnešní době X-band (7 – 8 GHz), Ku-band (11 – 18 GHz)

a Ka-band (20 – 30GHz). Všeobecně platí, že čím vyšší frekvence datového přenosu, tím je potřeba menší vyzářený výkon pro stejnou jednotku datového toku, avšak vysoké frekvence přenosu jsou velmi citlivé na přenosové prostředí (počasí, povětrnostní podmínky, viditelnost), a tím se snižuje jeho spolehlivost. Kromě jiných volitelných prvků spojení je zde také možnost volby přenosu datového paketu a modulace. Pro novodobé satelitní terminály je vhodné použít datový přenos TDMA a modulaci 8PSK

Z výše uvedených důvodů je tedy v návrhu komunikačního centra použito pásmo X-band, které disponuje vysokou spolehlivostí a odolností přenosu dat vůči přírodním faktorům.

Pro správnou konfiguraci, následnou funkčnost a monitorování satelitních terminálů je potřeba do místa nasazení nominovat satelitní tým techniků, který bude zajišťovat funkčnost prostředí po celou dobu nasazení.

Návrh satelitního přenosu dat do lokality komunikačního centra je zřejmý z obrázku 4.9.

4.1.3 Sekce RRL a rádiového přenosu

Sekce rádio-reléového (mikro-vlnného) a rádiového provozu bude v navrženém komunikačním centru hrát roli pouze záložního přenosu, proto ji v této podkapitole popisuji velmi zběžně. Je totiž známým faktem, že při provozování rádio-reléového datového toku potřebujeme pro spolehlivý a korektní přenos přímou viditelnost zářičů a maximální vzdálenost do 50 km. Proto lze toto spojení navrhnout pouze jako možnou alternativu mezi jednotlivými komunikačními centry v postižené oblasti. Páteřní datový přívod přes rádio-relé nemohu doporučit.

Schéma možného rádio-reléového datového spoje je zřejmé z obrázku 4.10.

Naopak antény pro rádiový přenos dat nepotřebují přímou viditelnost. Např. v pásmu KV (krátké vlny), kdy odraz vlny zajistí ionosféra, jsme schopni přenést signál přes velkou část zeměkoule. Velkým problémem je nízká průchodnost dat, proto ani použití rádiového provoz nemohu doporučit jako páteřní.

Pro primární datový tok je vhodná internetová linka od lokálního poskytovatele – viz podkapitola Sekce Network Exchange, pokud ovšem v místě nasazení taková možnost v krizové situaci existuje. Dalším primárním datovým tokem může být přenos satelitní – viz podkapitola výše.

4.1.4 Sekce Voice a VTC

Sekce Voice a VTC je dalším důležitou možností přenosu informací v rámci i vně navrhovaného komunikačního centra v době krizové události. Bez telefonie a videokonference se v dnešní době moderních technologií neobejde žádný nasaditelný prvek.

Přenos hlasu

Nejvariabilnější řešení telefonie v komunikačním centru je přenos hlasu pomocí konfigurovatelných digitálních IP telefonů, které můžeme připojit do jakéhokoliv síťového rozhraní PoE pomocí konektoru RJ45. Pro návrh telefonní sítě v komunikačním centru navrhuji použít IP telefon Cisco CP-8841, který je schopen se automaticky registrovat v CUCM *(Cisco Unified Communications Manager).* Po správné konfiguraci Call Manageru získá IP telefon přidělenou IP adresu z určeného podrozsahu a není nutné přístroj dále konfigurovat. Po zapnutí lze za pár vteřin telefonovat, popř. provozovat videohovor. Seznam kodeků, které přístroj podporuje, ukazuje jeho univerzálnost a možnost připojení i do jiných sítí, než Cisco (v případě potřeby).

Návrh sítě IP telefonie mezi komunikačními centry je zřejmý z obr. 4.1.

VTC – Videokonference

Pro vzdálené jednání při řešení úkolů, popř. artikulace problémů může být zapotřebí videokonferenčních hovorů. Pro samotný provoz navrhuji využití soupravy pro videokonference (např. Logitech), která není náročná pro instalaci, ani konfiguraci. Je kompatibilní se standardním PC přes USB, Wi-Fi, Bluetooth nebo NFC rozhraní. K videokonferenční soupravě je přiložen jednoduchý software pro zprostředkování spojení. V případě potřeby je zde možnost instalace jiného kompatibilního videokonferenčního software. Při používání videokonference je potřeba počítat s vyšším vytížením datové linky, proto doporučuji vytvoření rozpisu obsazení tzv. konferenční místnosti, která představuje přidělený datový tok. Omezení datového toku je nutno brát v potaz zejména v místě nasazení, kde nemusí být dostatečné přidělené datové pásmo pro obsluhu všech služeb. Schéma propojení podpůrných síťových prvků pro videokonferenci je zřejmé z obr. 4.12.

4.1.5 Sekce zřizování kabelových spojů a sítí

Důležitá oblast komunikačního centra je rovněž fyzická vrstva referenčního ISO/OSI modelu, což jsou kabelové spoje pro síťové prvky a koncová zařízení. V osádce obsluhy komunikačního centra v místě nasazení by určitě neměl chybět technik, který bude za funkčnost kabelové soustavy zodpovídat.

V základním rozdělení kabelů pro navrhované komunikační centrum se jedná především o kabely optické (z pohledu vláken jednovidové a mnohovidové) a o kabely UTP, popř. STP či FTP 5e generace s koncovkami RJ45.

Tyto základní druhy kabelů dokážou datově propojit téměř všechen komunikační a informační materiál *(CIS equipment)* navrhovaného komunikačního centra.

4.1.6 Sekce Monitorování a HelpDesk

Podstatnou částí fungování nepřetržitého provozu je zajištění směnnosti na sekci monitorování a Helpdesk (někdy také nazýváno Servicedesk). Popis této sekce komunikačního centra však patří do 5. kapitoly, kde se podrobně zbývám popisem zajištění provozu služeb komunikačního centra. V této kapitole je sekce monitorování a Helpdesku podrobně popsaná.

4.1.7 Sekce Network Exchange

Nedílnou součástí nasaditelného operačního centra je také sekce Network Exchange, která má zabezpečit a monitorovat konfigurace nasazených síťových prvků tak, aby koncové zařízení mohly být efektivně využívány dle potřeb post-krizových logistických procesů.

Níže detailně popíšeme návrh komunikačního centra na úrovni 1. fyzické, 2. linkové a 3. síťové vrstvě referenčního ISO-OSI modelu.

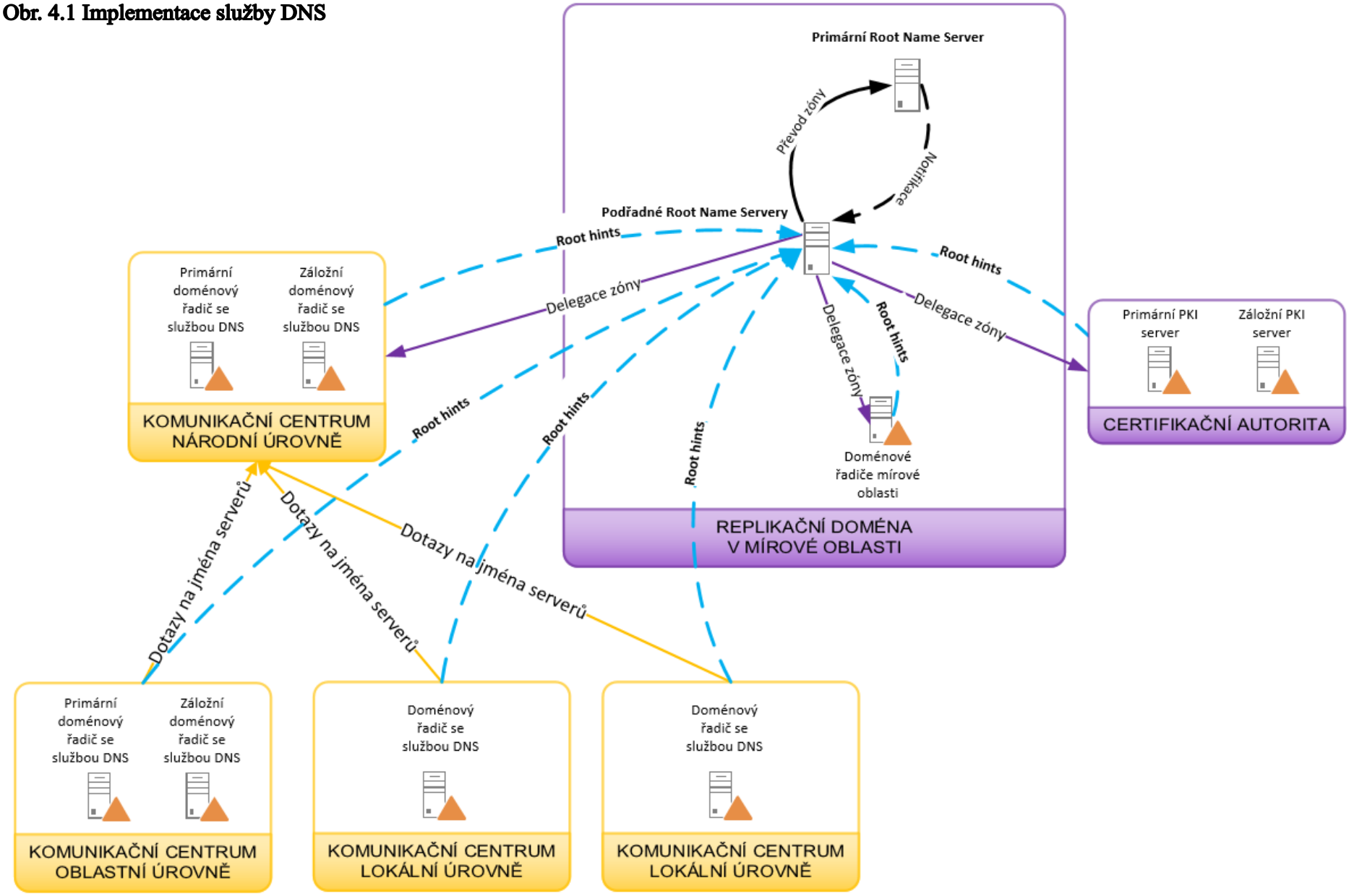
Mnou navrhované komunikační centrum má svůj hlavní páteřní router, který je hrdlem pro všechnu komunikaci vedoucí do a ven z uzlu. Je tvořen neutajovaným NU LAN routerem, popř. utajovaným UT LAN routerem, který slouží pro transformaci dat mezi jednotlivými komunikačními uzly, zabezpečující veškerý servis pro přenos prioritní komunikace a zaručující kompatibilitu spojení přes internetového poskytovatele. Komunikační centra vyšších úrovní obsahují 2 a více routerů spojené do klastru pro zaručení vysoce efektivní redundance. NU WAN ROUTER je schopen oddělit WAN části od LAN pomocí virtuálních rout (na jednom fyzickém routeru je možné vytvořit

několik virtuálních a plně oddělit jednotlivé komunikační zdroje) a přenášet data v zabezpečených šifrovaných tunelech do požadovaných destinací. Jedna z hlavních částí routeru je odpovědna za přenos komunikace mezi komunikačními uzly. (WAN komunikace). Další část vede data virtuálním routerem (NU VRF) směrem dovnitř uzlu pro celou neutajovanou komunikaci (LAN komunikace). Na hlavní část NU WAN ROUTERU je připojen ještě další router odpovědný za veškerý přenos utajované komunikace.
Schéma návrhu KC za sekci Network Exchange je zřejmé z obrázku 4.13.

4.1.8 Sekce utajení a kryptografie

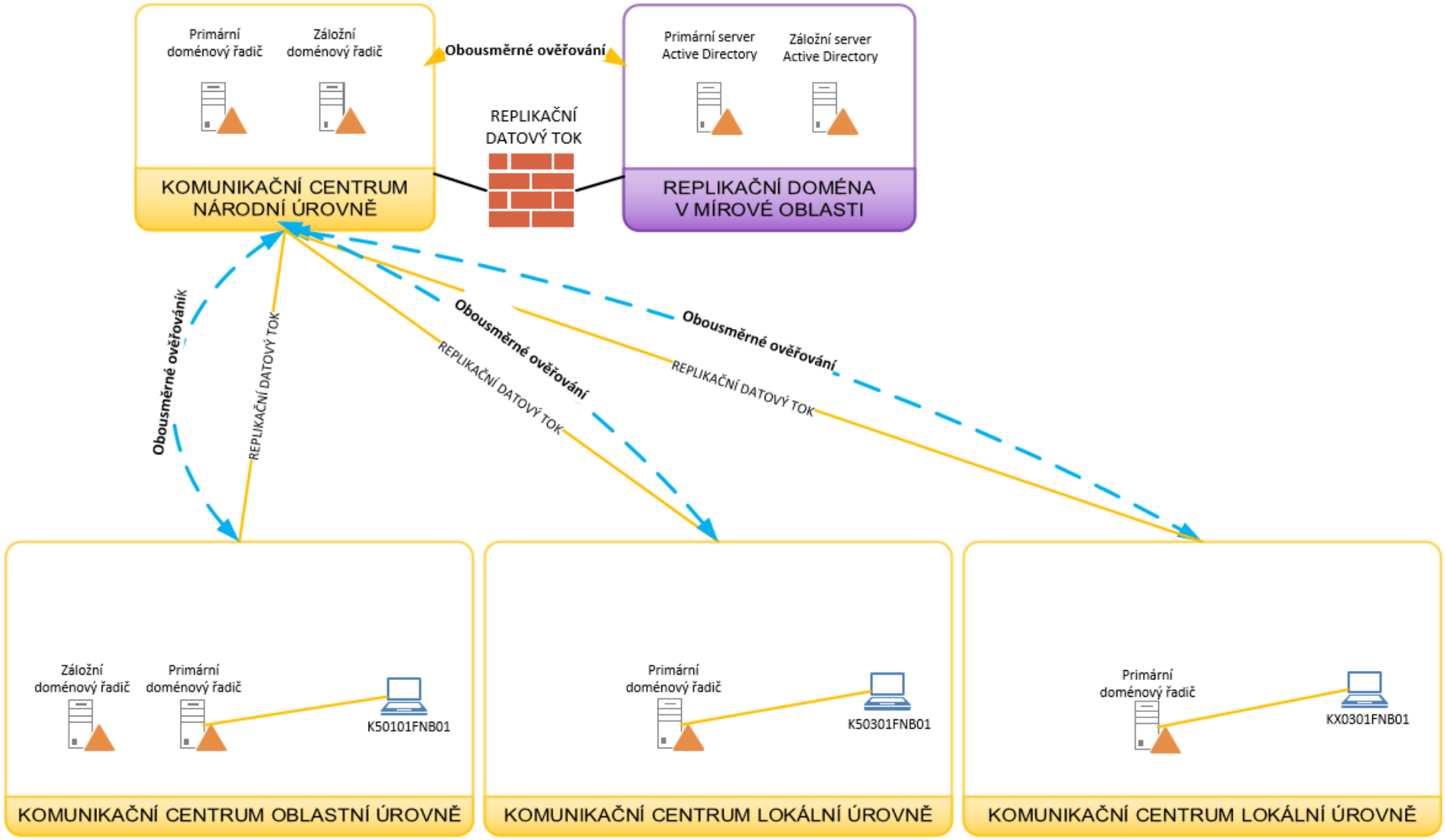
Z důvodu nutnosti implementace utajované části komunikačního uzlu je nutné zajistit adekvátní bezpečnostní standarty pro tuto komunikaci. Tato bezpečnost je zaručena pomocí fyzických šifrovacích zařízení, které zakódují veškerá data do neutajované části pomocí 2048 bitového kódu. Detailně tuto problematiku popisuji v příloze č. 6
Utajované a neutajované komunikační domény jsou rovněž znázorněny na obrázku 4.13.

Obr. 4.1 Implementace služby DNS



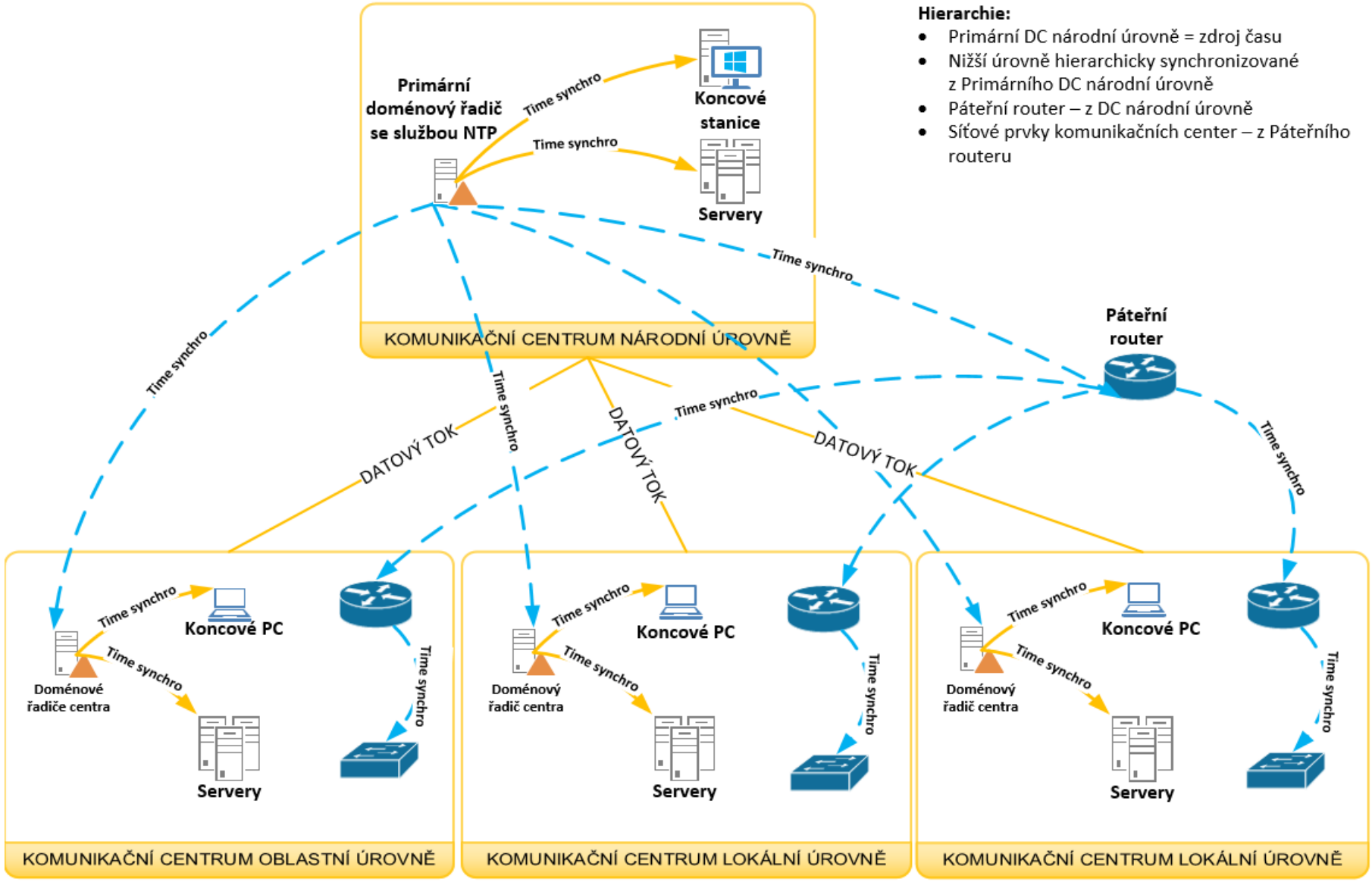
Zdroj: vlastní zpracování

Obr. 4.2 Implementace služby Active Directory



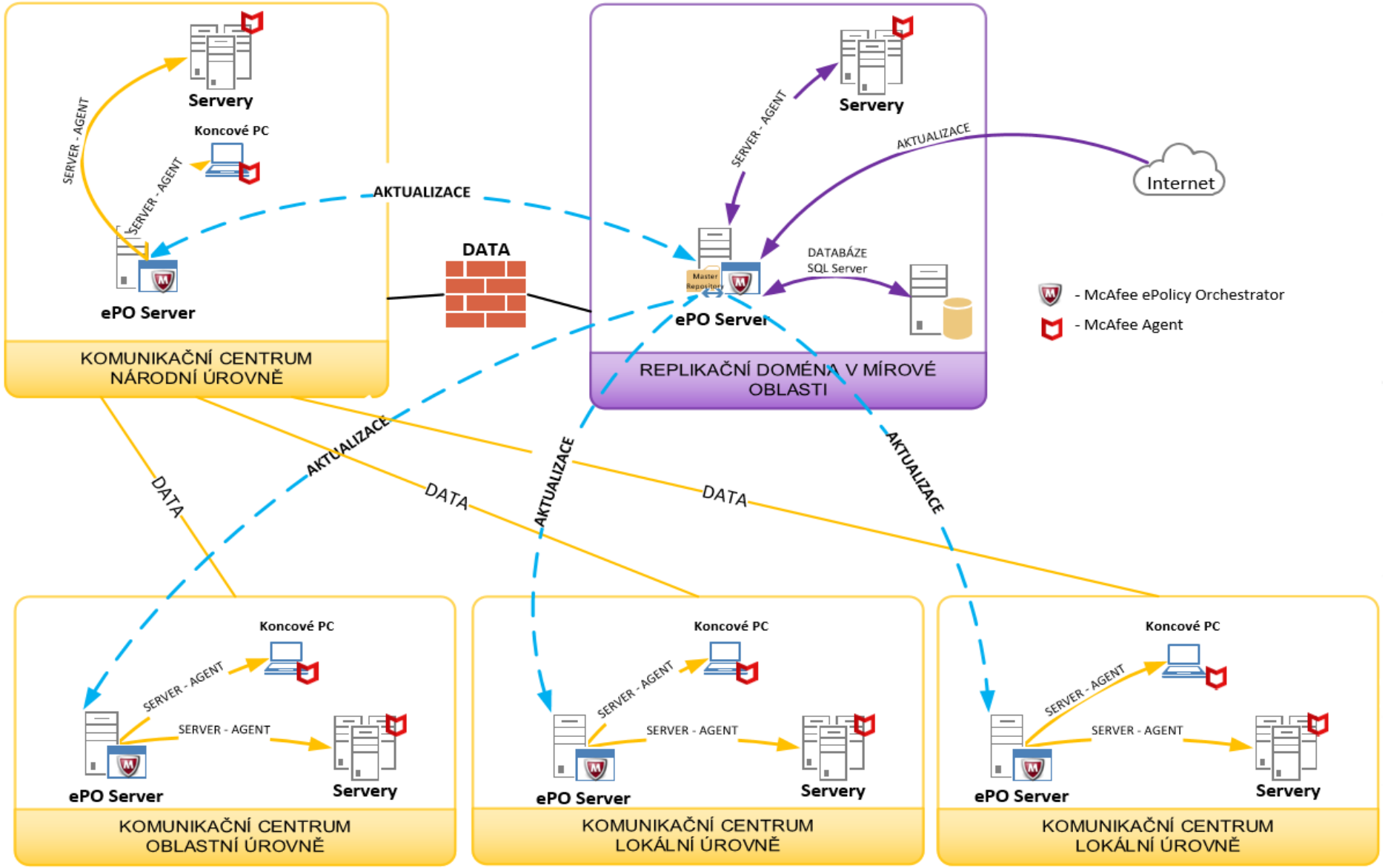
Zdroj: vlastní zpracování

Obr. 4.3 Implementace služby NTP



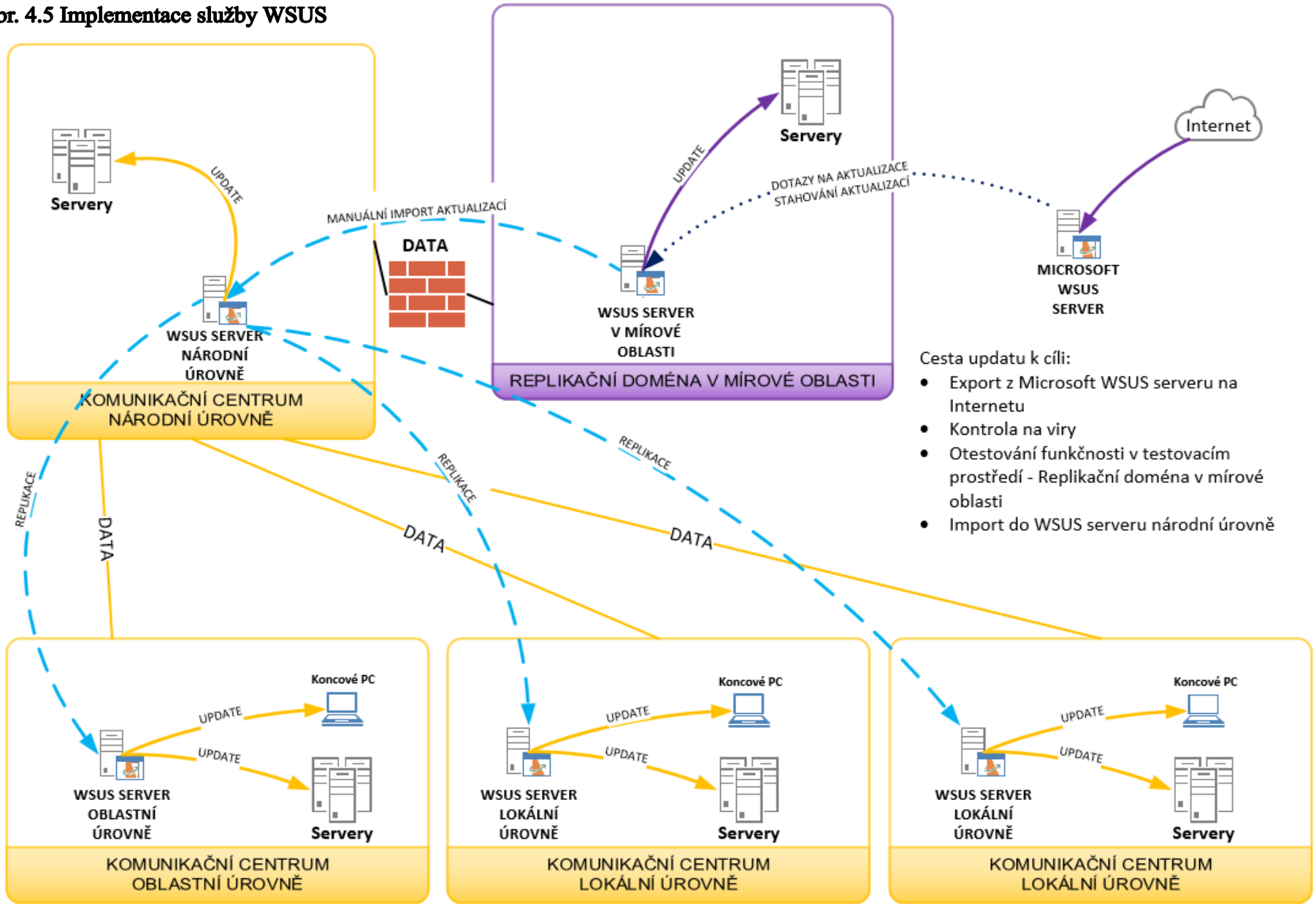
Zdroj: vlastní zpracování

Obr. 4.4 Implementace komplexní antivirové ochrany



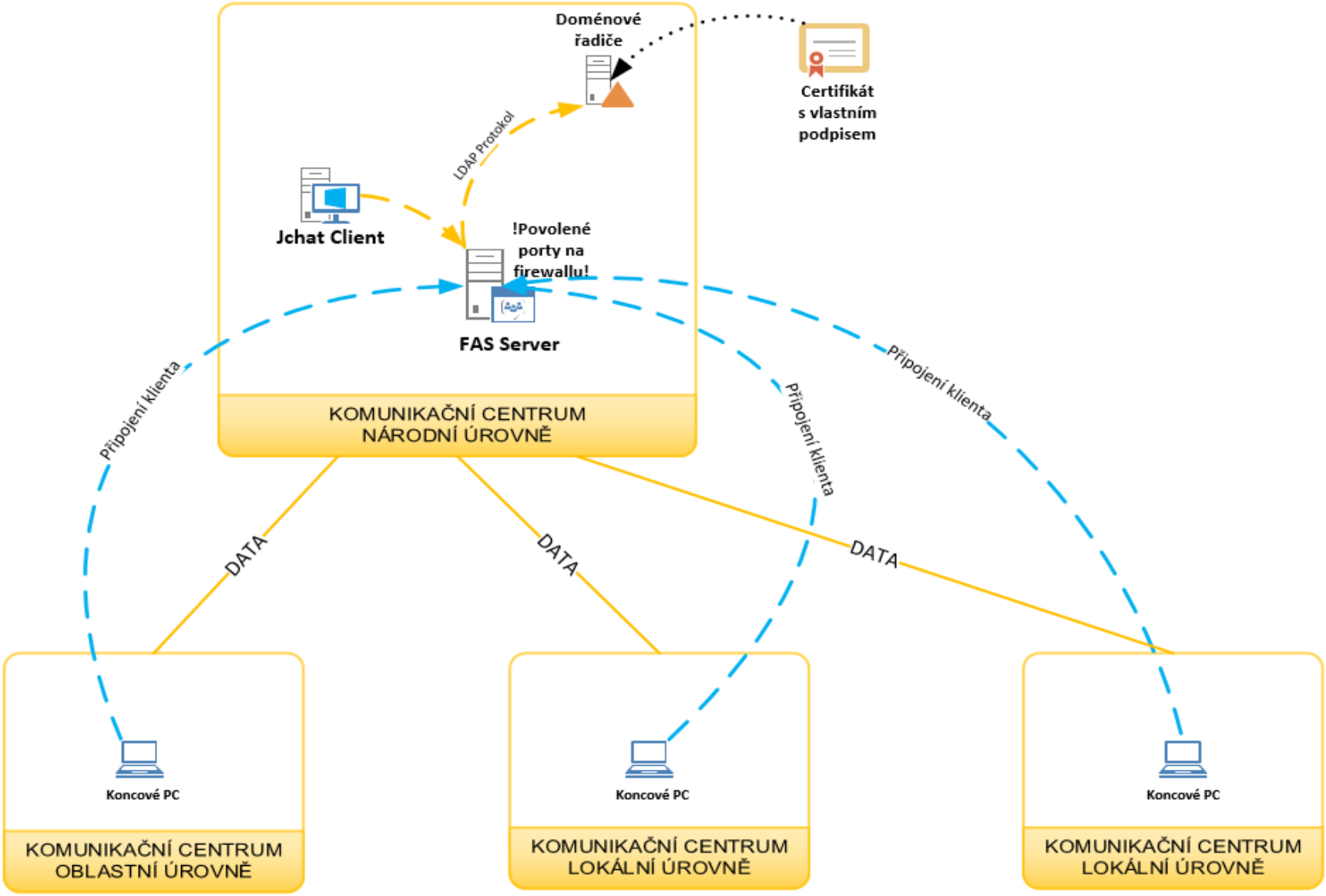
Zdroj: vlastní zpracování

Obr. 4.5 Implementace služby WSUS



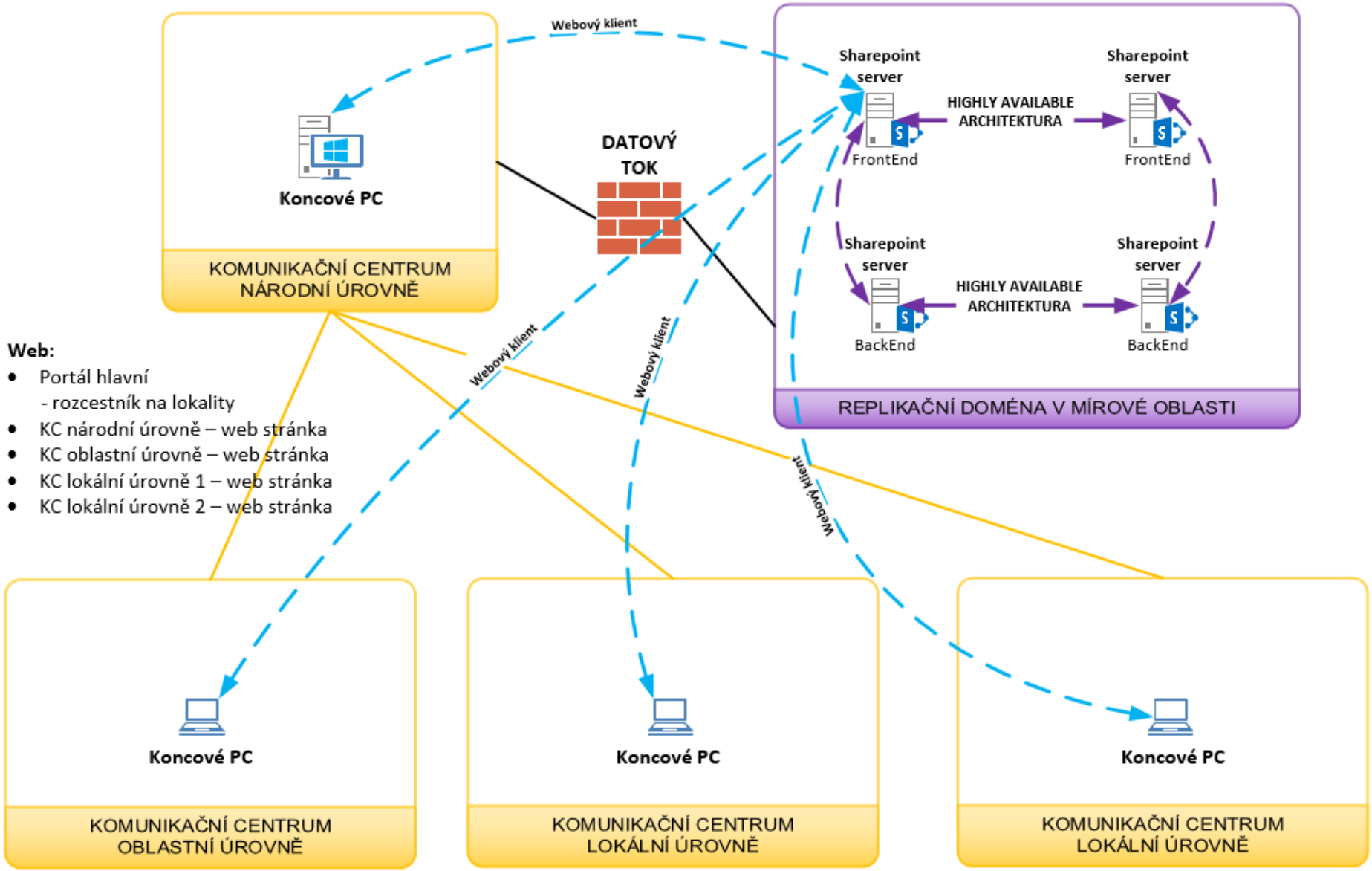
Zdroj: vlastní zpracování

Obr. 4.6 Implementace komunikačního klienta typu FAS



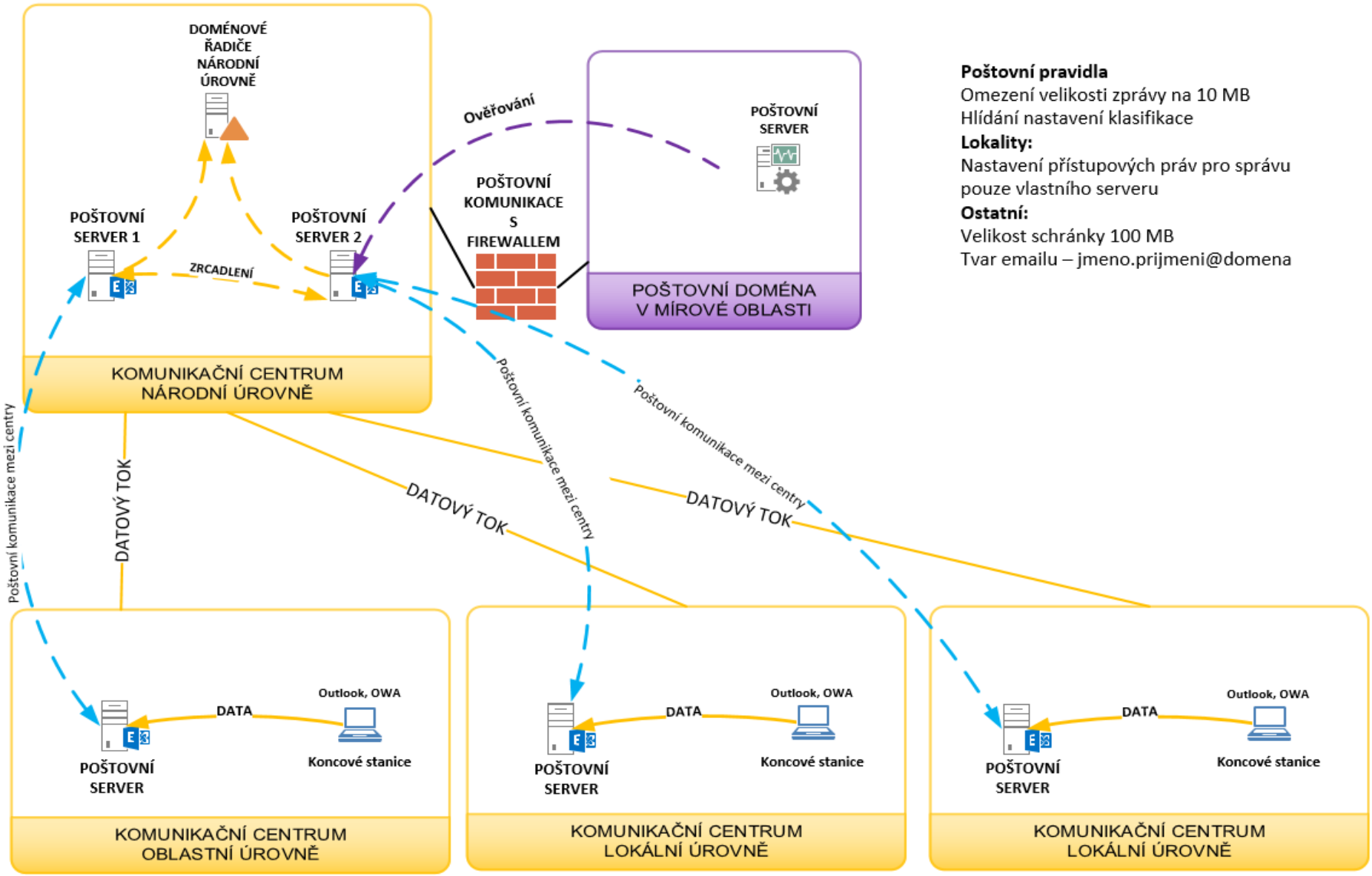
Zdroj: vlastní zpracování

Obr. 4.7 Implementace webového informačního portálu



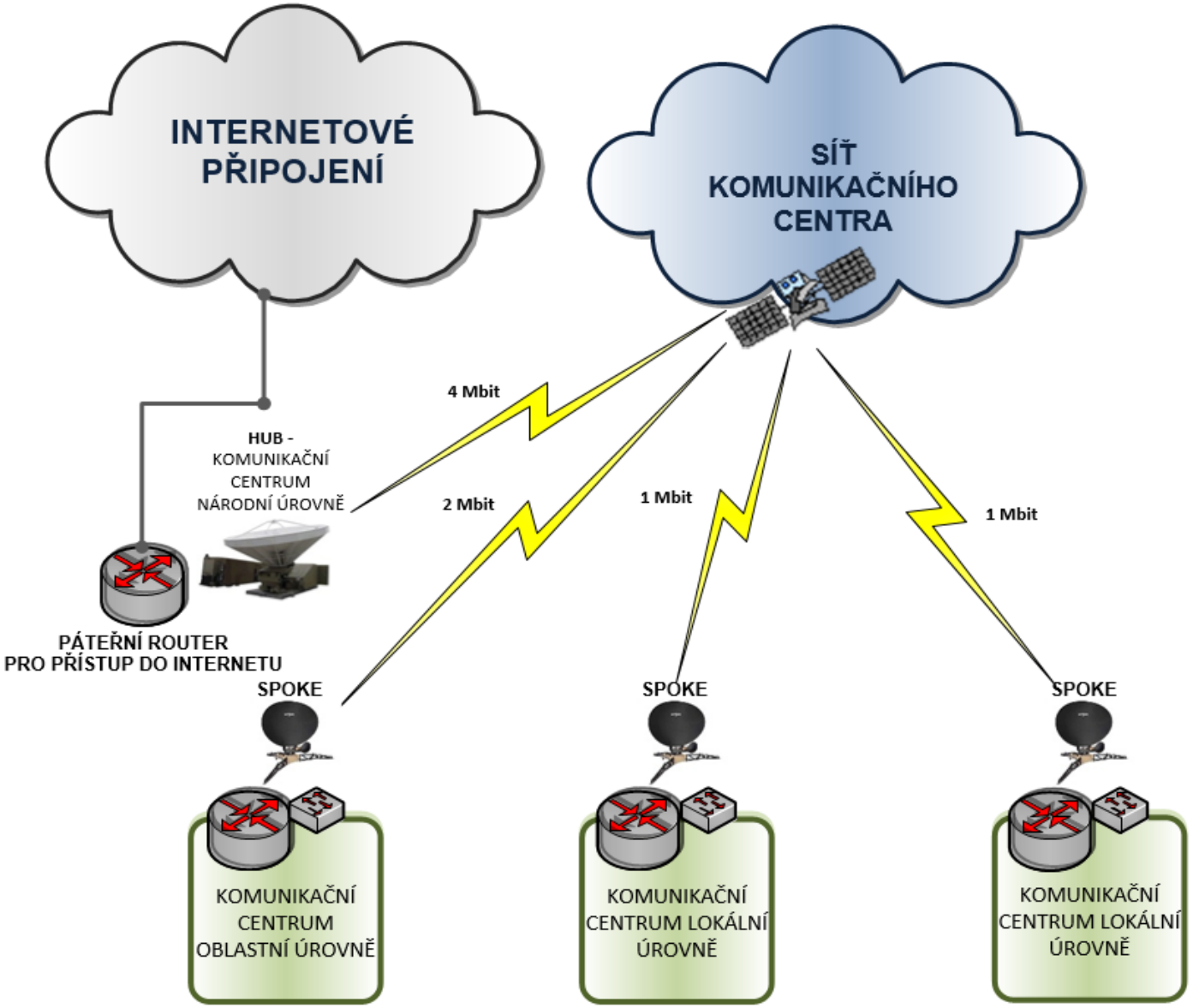
Zdroj: vlastní zpracování

Obr. 4.8 Implementace poštovní komunikace



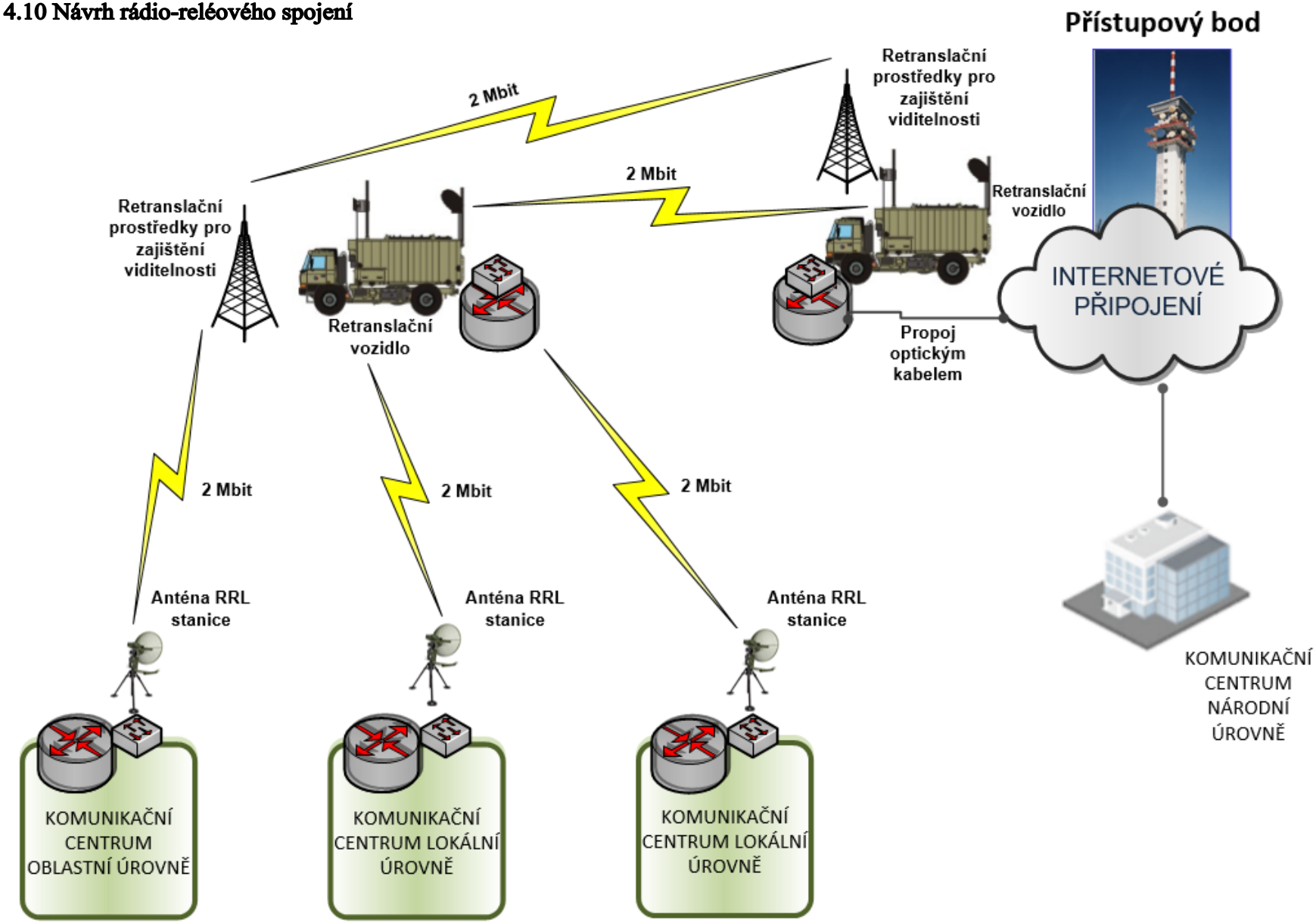
Zdroj: vlastní zpracování

Obr. 4.9 Návrh satelitního spojení



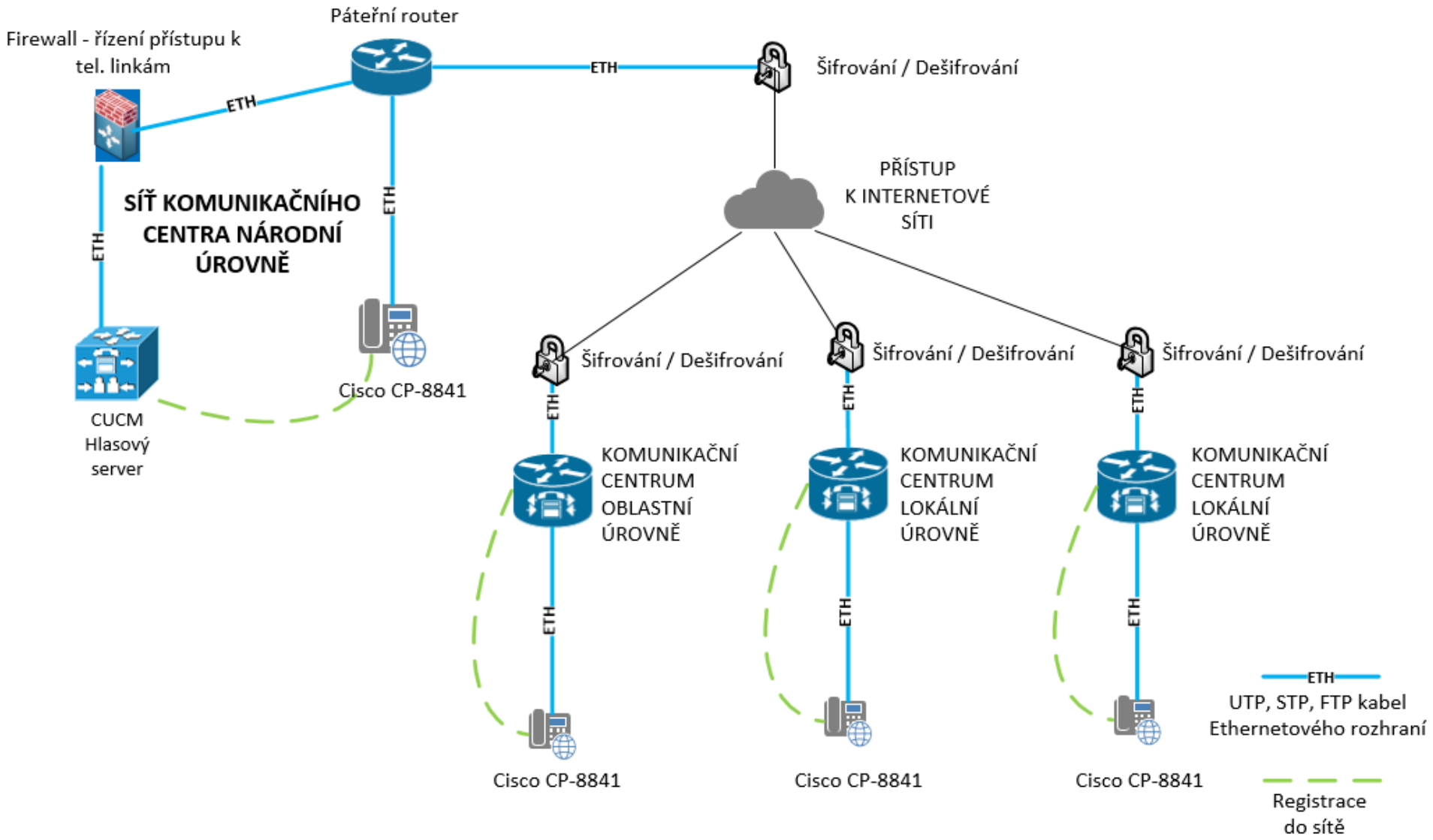
Zdroj: vlastní zpracování

Obr. 4.10 Návrh rádio-reléového spojení



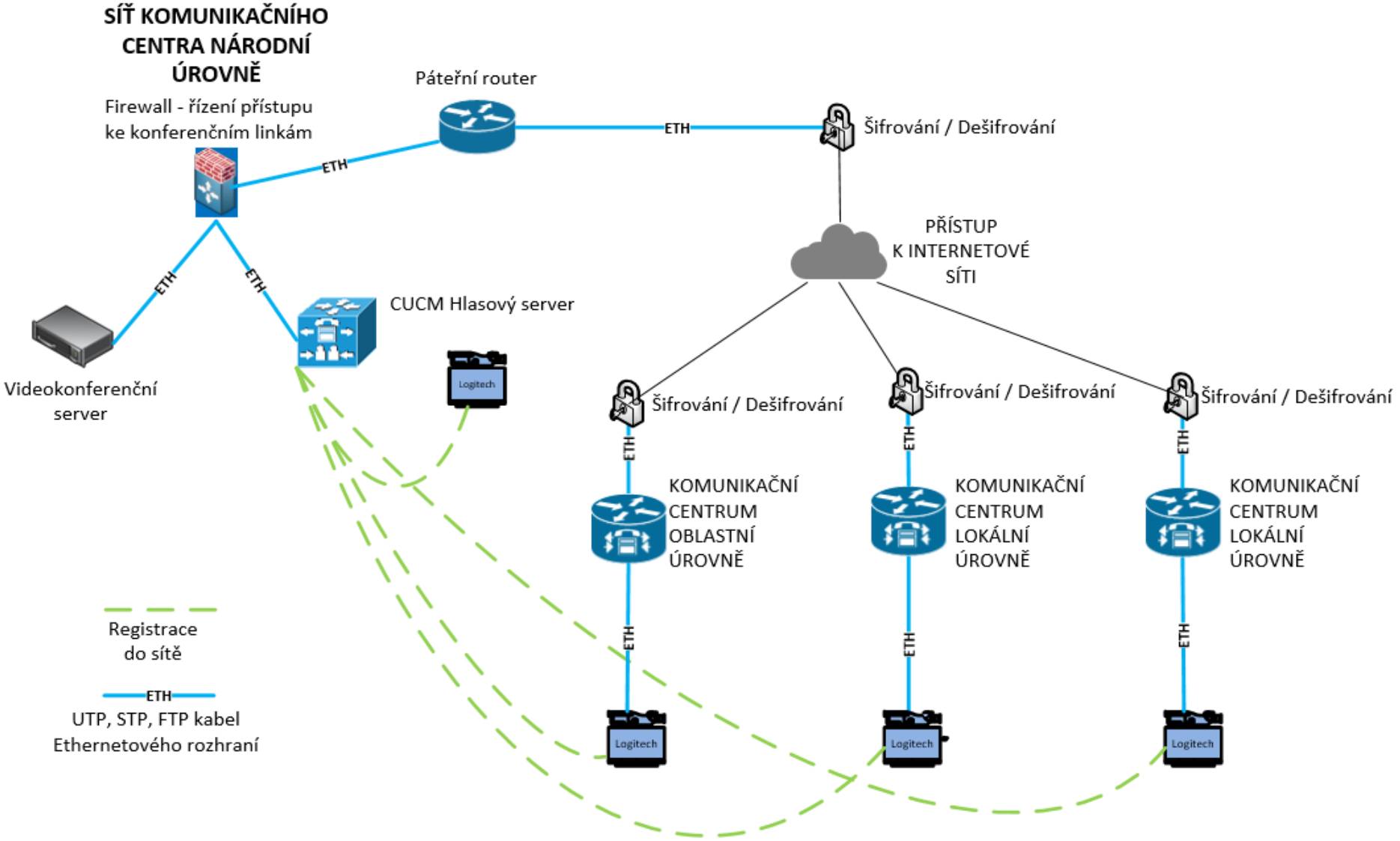
Zdroj: vlastní zpracování

Obr. 4.11 Návrh hlasové komunikace pomocí VoIP



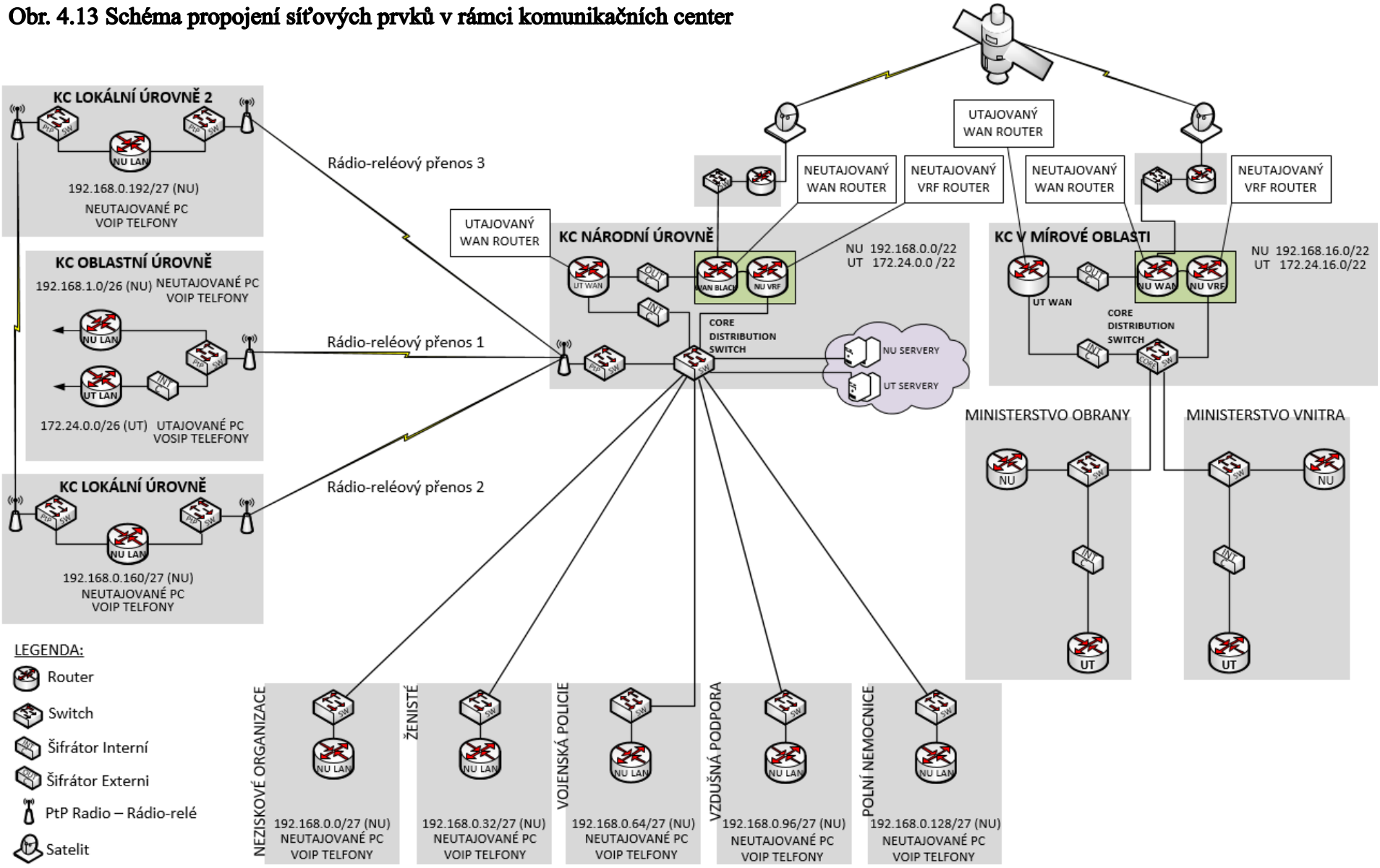
Zdroj: vlastní zpracování

Obr. 4.12 Návrh videokonferenční komunikace VTC



Zdroj: vlastní zpracování

Obr. 4.13 Schéma propojení síťových prvků v rámci komunikačních center



Zdroj: vlastní zpracování

4.1.9 Logistické zabezpečení komunikačního centra

Nyní krátce popíši prostředky a materiál, které si obsluha komunikačního uzlu vyváží do místa postiženého krizí. Pro nasazení komunikačního tělesa kdekoli ve světě počítám zejména s fází dopravy do místa nasazení a rozvinutí spojovacího uzlu do okamžiku zahájení nepřetržitého provozu.

Doprava do místa nasazení

Pro přesun materiálu a vybavení komunikačního navrhuji využití ISO 1C námořních kontejnerů o délce 20 stop (s vnitřními mírami: délka 5,898 mm, šířka 2,352 mm a výška 2,393 mm). K přepravě kompletního vybavení provedu výpočet váhy, případně objemu materiálu a vybavení nezbytného k zabezpečení úkolu a podle toho následně rozhodnu o počtu kontejnerů požadovaných pro přepravu. Při rozhodovacím procesu je nezbytné vědět jakou míru logistického zabezpečení je schopna zajistit hostitelská země. Vždy však počítám, že užitková voda a zdroj elektrické energie budou hostitelskou zemí poskytnuty v maximální možné míře. Při tomto výpočtu vycházím z předpokladů, že technologické zabezpečení uzlu včetně satelitních kompletů, klimatizací, záložních elektrocentrál a sudů s pohonnými hmotami vytvoří základní náklad v počtu 6 kontejnerů.

V případě, že jsem nucen spoléhat jen sám na sebe a veškerá logistická podpora bude organizována národní, nebo mezinárodní organizací, musím k přepravovanému materiálu připočíst také další pohonné hmoty, pitnou vodu, potraviny a nezbytný zdravotnický a hygienický materiál. Základními vstupními údaji jsou:

- Počet osob pro rozvinutí a provoz systému (pro mnou navrhovaný komunikační uzel se jedná o 25 osob)
- Spotřeba pitné vody na osobu a den (dle normy: 4,5 l na osobu a den)
- Spotřeba potravin na osobu a den
- 30 dní do nejpozdějšího dozásobení spotřebním materiálem

Pro výpočet zásob pitné vody a potravin vycházím ze základních jednotek, kterými jsou 4,5 l vody na osobu a den a jedna celodenní dávka potravin na osobu a den.

Pitná voda

Při 25 osobách se spotřebou 4,5 l na den a zásobě na 30 dní získávám jednoduchým násobením celkový počet 2250 PET balení o objemu 1,5 l. Jako přepravní balení využiji EURO paletu – viz obr. č. 4.14. Na jednu europaletu naskládám v jedné vrstvě 114 PET lahví což je 19 balení po šesti kusech. Tyto balení mohu naskládat až v pěti vrstvách, což činí 570 PET lahví na jednu paletu. Součtem zjistím, že pro přepravu pitné vody v požadovaném množství potřebuji v přepravním prostředku místo na 4 kusy EURO palet.

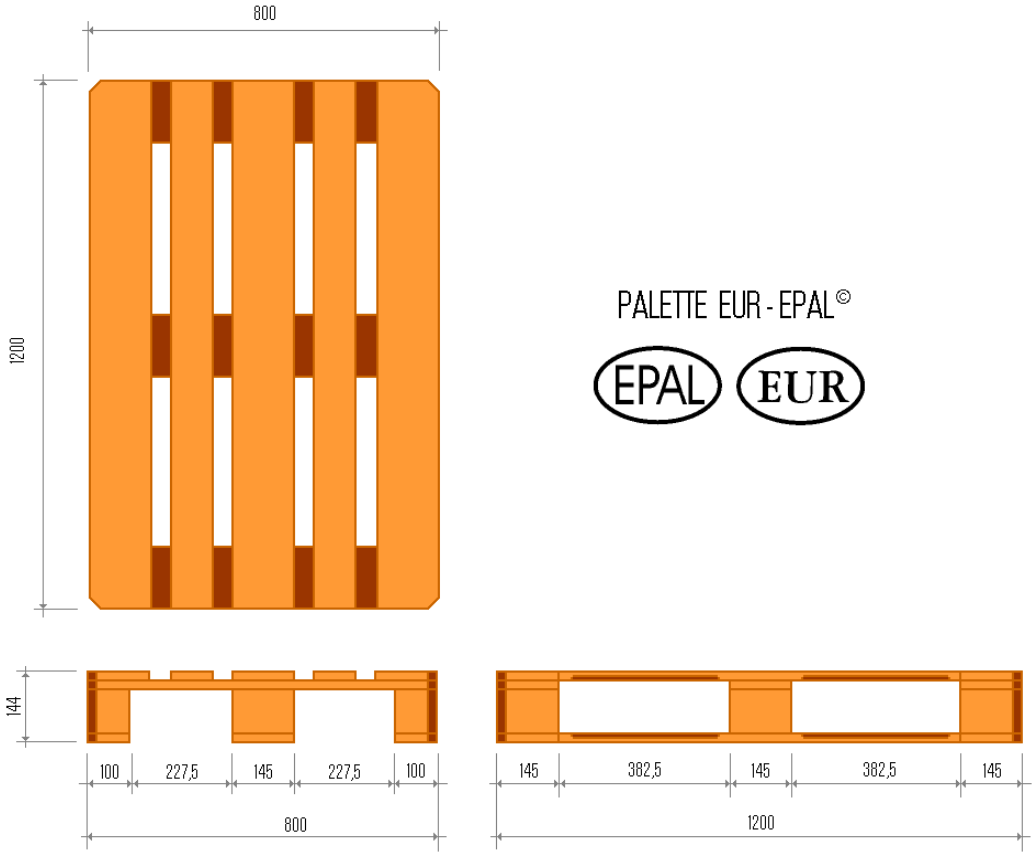
Potravinové dávky

Základními údaji jsou pro mne počet osob a dní, po které musím pro tyto osoby zajistit stravu. Násobkem získám celkový počet 750 denních potravinových balení. Tato strava je nejčastěji balená v krabici (25 mm x 11 mm x 19 mm) a je dodávána ve skupinovém balení po 10 ti kusech v třívrstvé klopové kartonové krabici s vnějšími klopami dna i víka doléhající k sobě bez překrytí, klopy jsou ve středové linii k sobě spojeny lepicí páskou. Toto skupinové balení má velikost 25 mm x 55 mm x 40mm. Použití EURO palety jako přepravního balení se tady přímo nabízí a vzhledem k velikosti krabic vím, že na paletu naskládám 20 kusů skupinových balení v celkem pěti vrstvách. K přepravě 75 kusů skupinových balení použiji celkem 4 EURO palety.

Vzhledem k velikosti ISO 1C kontejneru a použití EURO palet jako přepravního balení vím, že v kontejneru určeném pro přepravu pitné vody a potravin mám ještě místo pro tři EURO palety upevněné na podlaze kontejneru. Zbylý prostor je možné využít k přepravě osobního materiálu obsluhy. Obr. 4.15 ukazuje grafické vyobrazení možné nakládky EURO palet v kontejneru ISO 1C.

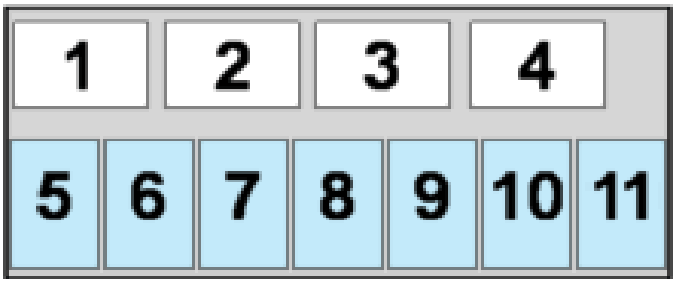
V případě nasazení tělesa komunikačního uzlu je vždy na hostitelské zemi, aby zajistila vhodné ubytovací kapacity pro obsluhu jednotlivých pracovišť na všech úrovních. Tedy přímo v blízkosti komunikačního uzlu a také ve všech ostatních místech, kde jsou dislokováni další pracovníci komunikačního uzlu (národní, oblastní centra).

Obr. 4.14 EURO paleta jako základní přepravní balení



Zdroj:[32]

Obr. 4.15 Grafické vyobrazení nakládky EURO palet v kontejneru ISO 1C



Zdroj: vlastní zpracování

5 ZAJIŠTĚNÍ PROVOZU SLUŽEB KOMUNIKAČNÍHO CENTRA

Služby poskytované komunikačním uzlem můžeme rozdělit do několika tříd

- Služby komunikační
- Služby informační
- Služby servisní

5.1 Služby komunikační

Komunikační služby poskytované v krizových řízeních zahrnují zejména služby linkového a bezdrátového hlasového spojení.

5.1.1 Linkové hlasové spojení

Pojem linkové hlasové spojení zahrnuje dva způsoby fonické komunikace. Základním požadavkem fonické komunikace je udržení snadno dostupného, stálého nepřerušovaného hlasového spojení mezi všemi koncovými zařízeními v telefonní síti.
První způsob je pro implementaci v krizovém řízení nepoužívaný modul analogového linkového spojení založeného na zřízení telefonní ústředny a roztažení linkového spojení k jednotlivým telefonním přístrojům.
Druhý způsob je dnes běžně využívaná oblast IP telefonie, která využívá stejnou síťovou architekturu a infrastrukturu jako v počítačové sítě, v místě krizového řízení.

5.1.2 Bezdrátové hlasové spojení

Bezdrátové hlasové spojení je dnes běžným celosvětovým standardem nejen pro krizové řízení na všech jeho stupních. Je založeno na přenosu signálu pomocí šíření elektromagnetického vlnění. Základním rozdělením bezdrátové fonické komunikace jsou technické prostředky, kterými je zabezpečeno. Podle toho dělíme rádiové spojení na Simplexní, poloduplexní a duplexní.

- **Simplexní** – radiostanice pracuje pouze s jednou frekvencí a může tedy být pouze v jednom ze dvou módů a to v módu přijímače, nebo vysílače.

- **Poloduplexní** – radiostanice pracuje se dvěma frekvencemi na ráz. Jedna frekvence je určena pro příjem signálu a druhá pro jeho vysílání. Radiostanice na opačné straně je naladěna opačně. I v tomto módu může stanice v jednom okamžiku provádět pouze jednu činnost, tedy buď vysílat, nebo přijímat signál. Takovými přístroji jsou v dnešní době běžně vybaveny jednotky integrovaných záchranných složek.
- **Duplexní** – radiostanice pracuje se dvěma frekvencemi, vysílací a přijímací. Může však pracovat s oběma módy naráz, takže v jednom okamžiku signál přijímá i vysílá. Na tomto principu funguje mobilní telefonie v systému GSM na několika základních frekvenčních pásmech (900, 1800 a 1900 MHz).

5.2 Služby informační

Informační služby jsou služby, které jsou uživateli poskytovány prostřednictvím jednotlivých koncových zařízení v počítačové síti. Zajištění fungování informačních služeb můžeme rozdělit do podskupin podle oblasti, kterými se jednotlivé služby zabývají. Jsou to služby aplikační, které zajišťují dostupnost a funkčnost programového vybavení. Služby síťové, které zajišťují provozuschopnost architektury počítačové sítě a všech jejích prvků. V neposlední řadě jsou to služby fyzické konektivity, které mají za úkol zabezpečení spojení mezi jednotlivými aktivními prvky v síti. Tedy neporušenost metalického a optického kabelového propojení a trvanlivost.

5.3 Služby servisní

Oblast servisních služeb je v rámci provozu komunikačního uzlu specifická požadavkem na lidskou obsluhu. Žádná s jejích složek se nedá realizovat bez lidské posádky. Do servisních služeb patří:

5.3.1 Servicedesk (Helpdesk)

Služba Servicedesk, někdy také zvaná Helpdesk je nepřetržitá služba prvního osobního nebo elektronického kontaktu uživatele komunikačních a informačních služeb s jejich poskytovatelem. Služba Servicedesk je pro poskytovatele komunikačních a informačních služeb nejnáročnější z hlediska lidské obsluhy. Je nezbytné, aby

fungovala v nepřetržitém provozu, a její náročnost je přímo úměrná počtu obsluhovaných uživatelů. Při počtu do padesáti uživatelů stačí k obsluze jedna osoba přes den a jedna pro noční směnu. Při počtu od padesáti do dvou set uživatelů je potřeba držet tuto službu přes den ve dvou osobách, zatím co v noci stačí osoba jedna. Nad dvě sta uživatelů je nezbytné, aby přes den službu obsluhovaly osoby tři a v nočních hodinách jedna. Počty osob ve směnách Servicedesku jsou samozřejmě také závislé na úrovni jazykových a odborných znalostí a zkušeností s prací v rámci dané služby.

Uživatel sem zpravidla přichází s požadavkem, který jasně definuje ve spolupráci s pracovníkem Service-desku. V zásadě se požadavky dají rozdělit na dva druhy:

- **Implementační** – uživatel požaduje po poskytovateli novou službu (zavedení nové telefonní linky, instalaci pracovní stanice, instalaci chybějícího softwarového vybavení, instalaci tiskárny, zřízení uživatelského účtu).
- **Změnový** – uživatel požaduje po poskytovateli změnu služby, která už byla implementována (resetování hesla, oprava pracovní stanice, oprava tiskárny, odebrání nebo výměna telefonu, odebrání nebo výměna pracovní stanice, výměna příslušenství pracovní stanice).

Poté co pracovník služby Servicedesk příjme požadavek uživatele, zaregistruje jej v informačním systému a službě Service management.

5.3.2 Service management

Service management je služba, která dále pracuje s požadavkem uživatele, analyzuje jej a určuje, která ze složek služby Service operation bude daný požadavek realizovat a také každému požadavku určí prioritu. V případě, že komunikační uzel zajišťuje služby jen malému počtu uživatelů, může být tato služba implementována přímo do služby Servicedesku.

5.3.3 Service operation

Service operation je souhrn jednotlivých služeb, které realizují požadavky koncových uživatelů. Patří sem zejména:

- **Výjezdová servisní skupina** – skupina zodpovědná za zajištění fyzických požadavků. Realizace připojení síťových prvků, instalace tiskáren a jejich připojení do sítě, provádění změn v datových a silnoproudých rozvodech, výměna pracovních stanic a jiných přístrojů. Z pohledu OSI modelu se jedná

zejména o zajištění služeb na fyzické a linkové vrstvě. Tato služba zpravidla není realizována v nepřetržitém režimu a jednotlivé úkoly jsou realizovány podle zadané priority.

- **Pracoviště dohledu nad síťovými prvky** – vzdálená kontrola jednotlivých aktivních síťových prvků (routery, switche) otevírání a zavírání jednotlivých portů při přidání nebo odebrání zařízení. Z pohledu OSI modelu se jedná o služby síťové a transportní vrstvy. Tato služba je vždy realizována v nepřetržitém provozu a to minimálně jednou osobou.
- **Pracoviště dohledu nad rádiovým a satelitním spojením –** obsluha komunikačních prostředků (rádiových stanic a vykrývačů signálu), která je zodpovědná za přidělování a řízení frekvencí pro rádiové sítě uživatelů na všech stupních krizového řízení. Za nepřerušované satelitní spojení s nadřízenými autoritami. S nástupem audiovizuálních komunikace je tato skupina pověřena řízením a organizací videokonferenčních spojení v utajovaných i neutajovaných doménách. V případě využití radioreléového point-to-point spojení mezi jednotlivými síťovými prvky, je tato skupina zodpovědná také za provoz těchto prostředků. Tato služba je vždy vedena nepřetržitým provozem a je zajišťována minimálně jednou osobou.
- **Pracoviště dohledu informačních systémů a aplikačního vybavení –** skupina administrátorů, která má za úkol pomocí vzdáleného přístupu zabezpečit funkcionalitu a dostupnost aplikačního vybavení instalovaného na jednotlivých pracovních stanicích, nebo serverech a to fyzických i virtuálních. Tato skupina zabezpečuje služby související s tvorbou editací a rušením účtů jednotlivých koncových uživatelů v různých doménách. Služba administrátorů je vždy vedena v nepřetržitém provozu a je zajišťována minimálně jednou osobou pro každou doménu. V případě krizového řízení se bude vždy jednat o dva správce uživatelských služeb.

ZÁVĚR

Stanoveným cílem diplomové práce bylo na základě návrhu výstavby a provozu komunikačního centra v podmínkách odstraňování následků přírodních katastrof resp. humanitárních krizí vytvořit funkční řešení v podobě konkrétního návrhu komunikačního centra, které bude schopné nasazení a interoperability v podmínkách přírodní katastrofy, popř. humanitární krize.

Čtenáře jsem podrobně seznámil s problematikou humanitární pomoci, mimořádných událostí a krizových situací v první a druhé kapitole této práce.

Ve třetí kapitole práce jsem se zaměřil na teorii nasaditelných komunikačních a informačních prostředků, které používá IZS. Konkrétní návrh zasazení potřebných služeb a přenosových systémů jsem podrobně popsal v kapitole č. 4, této práce, kde jsou jednotlivé přenosové prostředí graficky rozkresleny, ve schématech. Nasazení služeb jsem v návrhu rozdělil na úrovně provozu center, které jsou pro účely této práce rozděleny na národní, oblastní a lokální.

Zabezpečení nepřetržitého provozu a funkčnosti služeb je zprostředkováno pomocí stálé směny Service desku, jejíž popis pracovní náplně a zodpovědnosti jsem pak uvedl v kapitole č. 5.

Cílovou skupinou pro tuto práci je nasaditelná jednotka IZS, která bude vycvičená pro práci s komunikační a informační technologií, kde i znalost logistických procesů a použití techniky bude neméně důležité pro efektivní pomoc v postižené oblasti.

Návrh vybraného řešení byl vypracován na základě teoretických poznatků z odborné literatury, která se danou problematikou zabývá. Rovněž zde k návrhu přispěly i mé mnohaleté zkušenosti s nasaditelnou komunikační a informační technologií, která je používána například v misi Resolute Support v Afghánistánu a které mohou být v různých modifikacích uplatněny při řešení post krizových stavů kdekoli ve světě.

Můžeme tedy bez nadsázky napsat, že cíl práce byl splněn. Dokud se však toto řešení nedostane do rukou představitelů záchranných složek, výsledky nemůžeme zaručit. Podrobný výzkum a možnosti nasazení komunikačního centra nelze zachytit v rozsahu diplomové práce, proto si autor klade za cíl pokračovat v prohlubování znalostí v dané problematice při tvorbě disertační práce.

Soupis bibliografických citací

[1] PRAŽSKÝ STUDENTSKÝ SUMMIT. *Odstraňování následků humanitárních krizí* [online]. Praha: AMO, 2011 [cit. 5. 2. 2019]. Dostupné z: http://www.amo.cz/wp-content/uploads/2016/01/PSS-Odstraňování-následků-humanitárních-krizí-ECOSOC.pdf.

[2]CASTI, John. *Události X: možné scénáře kolapsu dnešního složitého světa.* Praha: Management Press, 2012. ISBN 978-80-7261-205-5.

[3] HENDRYCH, Tomáš. Termín krizová situace a jeho vymezení v krizovém řízení. In: *„112“, Odborný časopis požární ochrany, integrovaného záchranného systému a ochranyobyvatelstva.*Ročník VII, č. 6/2008.

[4] HASIČSKÝ ZÁCHRANNÝ SBOR ČR. *Krizové řízení* [online]. Praha: Generální ředitelství Hasičského záchranného sboru ČR, 2019 [cit. 14. 2. 2019]. Dostupné z: http://www.hzscr.cz/clanek/krizove-rizeni-oddeleni-krizoveho-rizeni-oddeleni-krizoveho-rizeni.aspx.

[5] KRULIŠ, Jiří. *Jak vítězit nad riziky: Aktivní management rizik – nástroj řízení úspěšných firem.* Praha: Linde, 2011. ISBN 978-80-7201-835-2.

[6] HASIČSKÝ ZÁCHRANNÝ SBOR ČR. *Havarijní plánování* [online]. Praha: Generální ředitelství Hasičského záchranného sboru ČR, 2019 [cit. 14. 2. 2019]. Dostupné z: http://www.hzscr.cz/clanek/menu-krizove-rizeni-a-cnp-krizove-a-havarijni-planovani-krizove-a-havarijni-planovani.aspx.

[7] GROSS, Ivan a kol. *Velká kniha logistiky.* Praha: Vysoká škola chemicko-technologická v Praze, 2016. ISBN 978-80-7080-952-5.

[8] DRAHOTSKÝ, Ivo a Bohumil ŘEZNÍČEK. *Logistika – procesy a jejich řízení.* Brno: ComputerPress, 2003. ISBN 80-7226-521-0.

[9] LAMBERT, Douglas M., STOCK, James R. a Lisa M. ELLRAM. *Logistika: příkladové studie, řízení zásob, přeprava a skladování, balení zboží.* 2. vyd. Brno: CP Books, 2005. ISBN 80-251-0504-0.

[10] HOLEJŠOVSKÝ, Jan. *Logistika a logistická podpora v krizovém řízení a ochraně obyvatelstva.* České Budějovice: Jihočeská univerzita v Českých Budějovicích, 2010. Diplomová práce.

[11] OSTRČILOVÁ, Kristina. *Mezinárodní humanitární pomoc a efektivnost charitativních sbírek na Haiti.* Brno: Masarykova univerzita, 2012. Diplomová práce.

[12] MINISTERSTVO ZAHRANIČNÍCH VĚCÍ ČR. *Humanitární pomoc – základní přehled*[online]. 2009 [cit. 13. 3. 2019]. Dostupné z: http://www.mzv.cz/file/501248/HPprehled.doc.

[13]MINISTERSTVO ZAHRANIČNÍCH VĚCÍČR. *Česká republika pomáhá*[online]. 2012 [cit. 14. 3. 2019]. Dostupné z: http://www.mzv.cz/file/876652/Ceska_Republika_Pomaha.pdf.

[14] HASIČSKÝ ZÁCHRANNÝ SBOR ČR. *Humanitární pomoc, to není jen pomoc materiální nebo finanční*[online]. 2012 [cit. 17. 3. 2019]. Dostupné z: https://www.hzscr.cz/clanek/humanitarni-pomoc-to-neni-jen-pomoc-materialni-nebo-financni.aspx.

[15] BARAN, Petr. *Informační technologie a informační systémy v krizovém řízení.* České Budějovice: Jihočeská univerzita v Českých Budějovicích, 2012. Diplomová práce.

[16] KARDA, Ladislav a Aleš KUDLÁK. *Analýza, metody a nástroje řešení krizových situací.* České Budějovice, 2007.

[17] HÁNA, Ivo. *Od analogových radiostanic k digitálnímu systému Pegas u HZS kraje Vysočina.* Ostrava: VŠB-TU, FBI, 2007. Bakalářská práce.

[18]INTV. *Spoje VSAT, satelitní telefony a terminály Inmarsat a Iridium* [online]. 2019 [cit. 13. 4. 2019]. Dostupné z: https://intv.cz/.

[19] SVATOŇOVÁ, Hana a Jaromír KOLEJKA. Geodatabáze v krizovém řízení. In *Informační systémy a technologie, základ interoperability krizového řízení ochrany obyvatelstva.* 1. vyd. Brno: MSD, 2007. s. 60-64. ISBN 978-80-86633-91-6.

[20]ADAMEC, Vilém a Luděk ŠTOLBA. *Informační technologie pro Integrovaný záchranný systém a krizové řízení*[online]. 2009 [cit. 4. 3. 2019]. Dostupné z: http://vsol.obce.cz/clanek.asp?id=2004307.

[21] MAŘÍK, Tomáš. Využití GIS aplikace v operačních střediscích emergentních složek. In *Požární Ochrana ´99.* Ostrava: VŠB-TU Ostrava a SPBI, 1999. s. 234-239.

[22] SOSINSKY, Barrie. *Mistrovství - počítačové sítě.* Praha: ComputerPress, 2010. ISBN 978-80-251-3363-7.

[23] ROSSI, Louis D., ROSSI, Louis R. a Thomas ROSSI. *Cisco& IP Addressing.* McGraw - Hill, 1999. ISBN 0-07-134925-1.

[24] DONAHUE, Gary A. *Network Warrior.* O´Reilly, 2011. ISBN 13-978-1449387860.

[25] TEARE, Diane a Catherine PAQUET. *Building Scalable Cisco internetworks (BCSI).* CiscoPress, 2007. ISBN 1-58705-223-7.

[26] LAMMLE, Todd. *CCNA Routing Switching Study Guide.* Sybex, 2013. ISBN 13-978-1118749616.

[27] PAVLOVEC, Michal. *Možnosti streamování datových proudů v lokálních sítích.* Ostrava: VŠB-TUO, 2018. Diplomová práce.

[28] WALLANCE, Kevin. CCNP Tshoot 642-832. Cisco Press, 2010. ISBN 10-1-58705-844-8.
[29] ODOM, Wendell. CCNP Route 642-902.CiscoPress, 2010. ISBN10-1-58720-253-0.

[30] CISCO NETWORKING ACADEMY. *Network Essentials* [online]. 2019 [cit. 12. 6. 2019]. Dostupné z: https://www.netacad.com/courses/networking/networking-essentials.

[31]KAZDA, Tomáš. *Technická infrastruktura a síťové technologie.* Praha: Bankovní institut vysoká škola Praha, 2012. Doplňkový studijní materiál kurzu se zaměřením na počítačové sítě.

[32] PALETÁRNA.CZ. *Dřevěná EUR paleta „A“ 120 x 80 nová* [online]. 2019 [cit. 24. 6. 2019]. Dostupné z: https://www.paletarna.cz/paletarna/Drevena-EUR-paleta-A-120-x-80-NOVA-d17.htm.

[33]ŠTRAUCHOVÁ, Zdenka. *Přes nový informační systém IZS již prošlo 100 milionů datových vět* [online]. 2016 [cit. 25. 6. 2019]. Dostupné z: http://www.nasepojizeri.cz/semilsko-aktualne/pres-novy-informacni-system-izs-jiz-proslo-100-milionu-datovych-vet/?aktualitaId=44105.

[34] HRADÍLEK, Ondřej. *Automatické ověření zaměřovací funkce letecké satelitní antény.* Brno: VUT, 2014. Diplomová práce.

[35] AVIT SYSTEMS. *Video Conferencing Solutions* [online]. 2012 [cit. 27. 6. 2019]. Dostupné z: http://avitsystemsinc.com/services/video_conferencing_solutions.

Použité legislativní zdroje

ČESKÁ REPUBLIKA. Zákon č. 239/2000 Sb., o integrovaném záchranném systému a o změně některých zákonů. In *Sbírka zákonů.* Praha: Parlament ČR, 2000, 73/2000, číslo 239. Dostupné také z: https://www.zakonyprolidi.cz/cs/2000-239.

ČESKÁ REPUBLIKA. Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů. In *Sbírka zákonů.* Praha: Parlament ČR, 2000, 73/2000, číslo 240. Dostupné také z: https://www.zakonyprolidi.cz/cs/2000-240.

ČESKÁ REPUBLIKA. Zákon č. 430/2010 Sb., kterým se mění zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů, ve znění pozdějších předpisů. In *Sbírka zákonů.* Praha: Parlament ČR, 2010, 149/2010, číslo 430. Dostupné také z: https://www.zakonyprolidi.cz/cs/2010-430.

ČESKÁ REPUBLIKA. Nařízení vlády č. 463/2000 Sb., o stanovení pravidel zapojování do mezinárodních záchranných operací, poskytování a přijímání humanitární pomoci a náhrad výdajů vynakládaných právnickými osobami a podnikajícími fyzickými osobami na ochranu obyvatelstva. In *Sbírka zákonů.* Praha: Vláda ČR, 2000, 132/2000, číslo 463. Dostupné také z: https://www.zakonyprolidi.cz/cs/2000-463.

ČESKÁ REPUBLIKA. Nařízení vlády č. 527/2002 Sb., kterým se mění nařízení vlády č. 463/2000 Sb., o stanovení pravidel zapojování do mezinárodních záchranných operací, poskytování a přijímání humanitární pomoci a náhrad výdajů vynakládaných právnickými osobami a podnikajícími fyzickými osobami na ochranu obyvatelstva. In *Sbírka zákonů.* Praha: Vláda ČR, 2002, 182/2000, číslo 527. Dostupné také z: https://www.zakonyprolidi.cz/cs/2002-527.

ČESKÁ REPUBLIKA. Zákon č. 151/2010 Sb., o zahraniční rozvojové spolupráci a humanitární pomoci poskytované do zahraničí a o změně souvisejících zákonů. In *Sbírka zákonů.* Praha: Parlament ČR, 2010, 53/2010, číslo 151. Dostupné také z: https://www.zakonyprolidi.cz/cs/2010-151.

ČESKOSLOVENSKÁ SOCIALISTICKÁ REPUBLIKA. Zákon České národní rady č. 133/1985 Sb., o požární ochraně. In *Sbírka zákonů.* Praha: Česká národní rada, 1985, 34/1985, číslo 133. Dostupné také z: https://www.zakonyprolidi.cz/cs/1985-133

ČESKÁ REPUBLIKA. Zákon č. 238/2000 Sb., o Hasičském záchranném sboru České republiky a o změně některých zákonů. In *Sbírka zákonů.* Praha: Parlament ČR, 2000, 73/2000, číslo 238. Dostupné také z: https://www.zakonyprolidi.cz/cs/2000-238

Seznam zkratek a terminologie

AD – Active Directory

AP - Přístupový bod (Access point)

ARS – Analogová rádiová síť

ASŘ – Automatizace systému řízení

BDC – Backup Domain Controller

BOZP – Bezpečnost a ochrana zdraví při práci

CUCM – Cisco Unified Communications Manager

DC – Doménový řadič (Domain Controller)

DHCP - Dynamic Host Configuration Protocol

DNS – Doménový server (Domain Name Server)

EU – Evropská Unie

FAS - Functional Area Services

HDD – Pevný disk (Hard drive)

http – Hypertext Transfer Protocol - je internetový protokol sloužící pro výměnu hypertextových dokumentů ve formátu HTML

https – Hypertext Transfer Protocol Secure - bezpečná verze hypertextového přenosového protokolu, přenášená data jsou kódovaná protokolem SSL nebo TLS

IZS – Integrovaný záchranný systém

KV - krátké vlny

LAN – Local Area Network

MAN – Metropolitan Area Network

MU - Mimořádná událost

MV – Ministerstvo vnitra

NATO – Severoatlantická aliance (North Atlantic Organisation)

NTP – Network Time Protocol

OSN – Organizace spojených národů

PAN – Personal Area Network

PDC – Primary Domain Controller

PoE – Power of Ethernet

RRL - rádio-reléové spojení

SCCM - System Center Configuration Manager

STP - stíněné kroucené páry (Shielded Twisted Pair), které mají mezi páry a vnějším pláštěm celistvý hliníkový obal, který se na koncích uzemní a tím se zamezí vniknutí rušení.

TDMA – Time Division Multiple Access

UTP – nestíněné kroucené páry (Unshielded Twisted Pair), které díky svým vlastnostem eliminují vlivy okolního elektromagnetického rušení

VLAN – Virtual Local Area Network

VoIP – Voice over Internet Protocol

WAN – Wide Area Network

WSUS - Windows Server Update Services

Seznam ilustrací a tabulek

Seznam příloh a přílohy

Příloha č. 1 - Vývojový cyklus krize

Z hlediska míry ohrožení nedosahuje většina mimořádných událostí hranice krize. Tyto události představují lokální, ohraničenou zátěž, která je v daném prostředí a čase zvládnutelná (např. možnostmi integrovaného záchranného systému), takže se nestává zdrojem nestability pro své okolí (např. provozní nehody). Není naplněna jevová stránka krize, i když důsledky takovéto události mohou být tragické.

Jinak je tomu, když se vlivem mimořádné události jevová stránka krize naplní. Stane se tak, když mimořádná událost nezůstává jen situací „samou o sobě“, ale je spouštěčem této krize.

Krize se vyvíjí **v časově ohraničených fázích**, které tvoří vývojový cyklus krize. Tento známý poznatek (převzatý z ekonomie) platí obecně pro krize z různých zdrojů v různých prostředích.[…]

Fáze elevace je počáteční fází krize (identická s časovým úsekem t0-t1), kdy se nestabilita prostředí vznikem a vlivem mimořádné události zvyšuje, kdy se mimořádná událost jako potenciální zdroj krize projevuje sílicími dopady a kdy při nepřijetí dostatečných opatření k obnovení stability dochází k eskalaci krize (nárůstu a zmnožení ohrožení). Ne vždy se ale elevace výrazně projeví.

Fáze eskalace je pokračující fází krize (identická s časovým úsekem t1-t2), kdy tím, že není dosaženo stability, ohrožení narůstá. Mimořádná událost – jinak zdroj krize – vyvolá další mimořádné události v jiných prostředích (méně stabilních), přičemž dochází k prudkému, stupňovitému nárůstu nestability. Dopady mimořádných událostí sílí, zvyšuje se jejich četnost a závažnost.

Fáze kulminace navazuje na předchozí fázi krize (je identická s časovým úsekem t2-t3). V ní krize dosahuje svého vrcholu (úrovně kritického bodu), přičemž ve sledovaném prostředí dochází ke zpomalení až zastavení růstu intenzity ohrožení.

Délka fáze kulminace může být relativně velmi krátká. V extrémním případě může být tato délka z časového hlediska zanedbatelná, může se jednat jen o okamžik vyvrcholení krize, např. o přechod průlomové vlny po protržení hráze“.

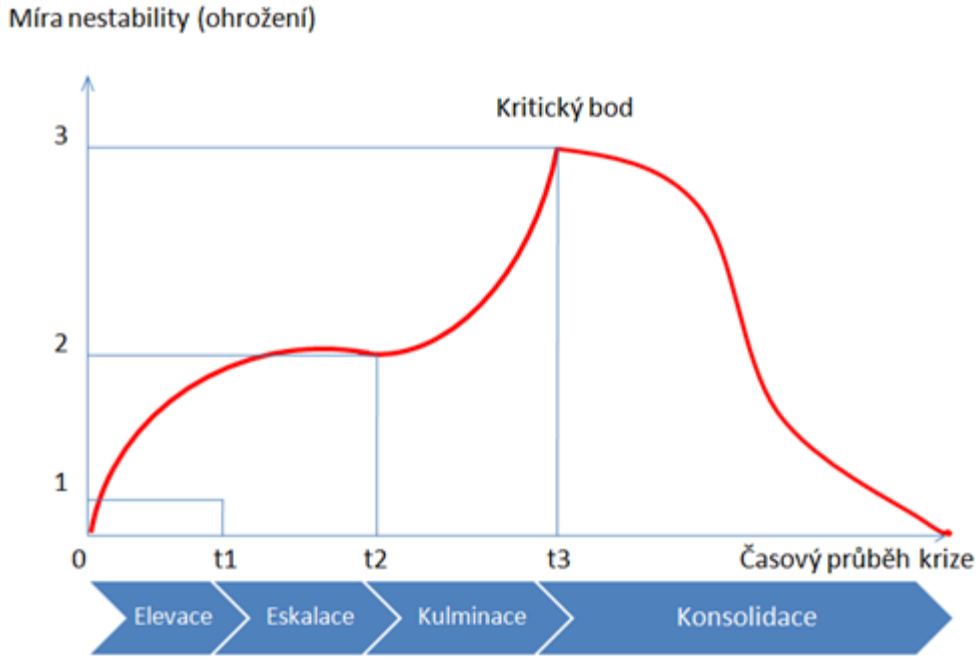
Fáze kulminace může být i při dočasném zamezení rozrůstání krize mezistupněm pro její další eskalaci.

Fáze konsolidace je fází krize po zastavení působení ohrožení (identická s časovým úsekem t3 – t4). Pro fázi je charakteristické zapojení do činností k dosažení relativně

trvalé stability prostředí s novými hranicemi stability. Jedná se o aktivity ke standardizaci běžného života, odstraňování škod atd. [3].

Vývojový cyklus krize znázorňuje také obrázek P1.1.

Obr. Příloha 1.1 Vývojový cyklus krize



Zdroj: [3]

Probíhající krize, odezva a obnova

Z jednotlivých fází vývojového cyklu krize lze dovodit, jaký význam mají v průběhu krize „stabilizační síly“ a jaká je jejich funkce. K tomu poslouží přiblížení pojmů odezva na krizovou situaci a obnova.

Odezva na krizovou situaci je souborem opatření za účelem zvládnutí krizové situace, tzn. dosažení stability v daném prostředí a jeho okolí a zamezení nebo omezení dalšího rozvoje negativních dopadů.

Obnova znamená soubor opatření k vypořádání se s důsledky krizové situace, k zajištění a udržení stability, k likvidaci škod a k nastoupení dalšího rozvoje.

Přináležitost odezvy a obnovy k jednotlivým fázím vývojového cyklu krize nelze s přesností ohraničit. Z hlediska své podstaty se odezva více realizuje v počáteční a postupných fázích krize (koordinací řízení, zásahy k potlačení mimořádných událostí, silami a prostředky), obnova pak v závěrečné fázi. Opatření odezvy a obnovy se časově překrývají [3].

Krizová situace a krizový stav

Z uvedeného vyplývá, že krizová situace je mimořádnou událostí, která neudržitelně roste jako zdrojová buď samostatně, nebo se spolupůsobením dalších mimořádných událostí. Vzniká, rozrůstá se a trvá vždy v určitém prostředí a společenství podle toho, zda jsou a jak zasáhnou nástroje stabilizace, tj. zda bude přijata odpovídající odezva (mj. i vyhlášení krizového stavu příslušným orgánem krizového řízení). Například chudě institucionální společnost potřebné nástroje vůbec nemusí mít. Znamená to konečně, že jako krizovou situaci nelze výlučně označovat jen událost, při níž je vyhlášen krizový stav.

Vyhlášení krizového stavu je především právní kategorií pro zvládání krizové situace. Umožňuje orgánům krizového řízení zavést krizové postupy a opatření v přímé závislosti na charakteru a rozsahu krizové situace (obvykle zákonné povinnosti, zákonná omezení a zákonnou regulaci). Ve vývojovém cyklu krizové situace je vyhlášení krizového stavu aktem elevace, maximálně eskalace.

Pro stručné a výstižné vyjádření pojmu krizová situace v zákoně lze z předchozího textu generovat:

Krizová situace je mimořádná událost nebo mimořádné události, které velikostí a rozsahem ohrožení způsobují destabilizaci určitého prostředí a společenství, a vyžadují zavedení stabilizačních opatření na jednotlivých stupních veřejné správy [3].

Oddělení krizového řízení při přípravě na krizové situace a jejich řešení plní zejména tyto úkoly:

- organizuje součinnost v oblasti krizového řízení mezi správními úřady a obcemi v kraji,
- zpracovává krizový plán kraje a krizový plán obcí s rozšířenou působností,
- vede přehled možných zdrojů rizik a provádí analýzy ohrožení,
- zpracovává havarijní plán kraje a vnější havarijní plány,
- vyžaduje, shromažďuje a eviduje údaje nezbytné ke zpracování krizového plánu kraje a obce s rozšířenou působností,
- podílí se na provádění vzdělání v oblasti krizové a havarijní připravenosti,
- připravuje a usměrňuje zpracování podkladů pro jednání bezpečnostní rady kraje,
- vykonává státní správu na úseku prevence závažných havárií,
- plní úkoly v oblasti kritické infrastruktury a její ochrany,

- vytváří podmínky pro činnosti krizového štábu kraje a obcí s rozšířenou působností a podílí se na zabezpečení jejich činnosti,
- vytváří podmínky pro činnosti štábu HZS a operačních skupin HZS ÚO a podílí se na zabezpečení jejich činnosti,
- podílí se na plnění úkolů v oblasti hospodářských opatření pro krizové stavy, za tím účelem vyžaduje, shromažďuje a eviduje údaje o nezbytných dodávkách a dodavatelích v informačním systému ARGIS,
- seznamuje obce s rozšířenou působností a právnické nebo fyzické osoby na jejich žádost s charakterem možného ohrožení, s připravenými krizovými opatřeními a se způsobem jejich provedení,
- vykonává kontrolu v oblasti krizového řízení u obce s rozšířenou působností, obce a právnických osob a podnikajících fyzických osob, kterým uložil povinnost vyplývající z krizového plánu,
- plní další úkoly stanovené v rámci přípravy a ve prospěch řešení krizových situací [4].

Příloha č. 2 - Řízení pomoci – průběh humanitárních projektů v praxi

Pro dotační výběrová řízení na humanitární pomoc jsou stanovena tato **kritéria pro posuzování návrhů projektů**:

Formální náležitosti projektu:

- Úplnost uvedených údajů,
- Kvalita a jasnost uvedených údajů.

Relevance:

- Relevance ke konkrétním potřebám postižené země a jejího obyvatelstva,
- Relevance k mezinárodním principům humanitární pomoci a prioritám humanitární pomoci ČR (důraz na záchranu životů a zmírňování utrpení, pomoc při návratu k normálnímu životu, nestrannost, neutralitu, rovnost žen a mužů, respektování mezinárodního humanitárního práva a lidských práv).

Přínos projektu:

- Do jaké míry projektové zdroje a zvolené strategie citlivě a účinně přispívají k dosažení předpokládaných cílů,
- Jasná specifikace cílů a výstupů projektu.

Účelnost:

- Přiměřenost nákladů k očekávaným výstupům,
- Využití jiných zdrojů financování (žadatel, jiný donor).

Udržitelnost:

- Míra participace místní komunity na plánování a realizaci projektu,
- Pravděpodobnost návaznosti dalších aktivit na přínosy projektu (projekty rozvojové spolupráce, zapojení jiného donora).

Organizační zajištění:

- Dosavadní zkušenost realizátora s poskytováním humanitární pomoci,
- Zkušenosti realizátora z regionu/teritoria,
- Existence administrativního zázemí v místě realizace, spolupracující partnerská organizace v místě realizace,
- Míra koordinace s ostatními poskytovateli humanitární pomoci [11].

Součinnost ve financování mezinárodní humanitární pomoci mezi veřejnou správou a neziskovým sektorem v ČR

Spolupráce neziskového sektoru a veřejné správy je nezbytnou podmínkou zefektivnění celého procesu pomoci. Jak již bylo pojednáno v předešlých kapitolách, způsoby pomoci jsou mnohé.

Pokud však zůstaneme u organizování humanitární pomoci do zahraničí, můžeme říci, že Česká republika tuto pomoc zprostředkovává díky NGO (českým i mezinárodním) a mezinárodním vládním organizacím. Z velké části jde o poskytnutí finančních zdrojů. Dvěma hlavními aktéry v oblasti státní správy jsou Ministerstvo zahraničních věcí a Ministerstvo vnitra. Dle zákona č. 151/2010 Sb., o zahraniční rozvojové spolupráci a humanitární pomoci by měla být státům Evropské unie a Evropského hospodářského prostoru poskytována humanitární pomoc (nyní myšleno finanční) Ministerstvem vnitra, ostatním zemím pak Ministerstvem zahraničních věcí. Nicméně *„v praxi existuje zatím pouze jeden rozpočet, který je v gesci MZV.“* Spolupráci (včetně poskytování dotací) s výše zmíněnými organizacemi zabezpečuje Odbor rozvojové spolupráce a humanitární pomoci MZV [11].

Oficiální rozvojová pomoc (ODA), jakožto finanční pomoc z veřejných rozpočtů České republiky (zejména rozpočtu MZV), má pro efektivnější poskytování humanitární pomoci do zahraničí důležitý význam. ODA je tvořena z finančních prostředků vynaložených pouze do *„započitatelných zemí“*, tedy rozvojových. Z tohoto důvodu se například humanitární pomoc pro Japonsko do ODA nezahrnuje. Oficiální rozvojová pomoc není určena jen pro neziskové organizace. Je často zmiňována v souvislosti s mnohostrannou pomocí, kdy jsou finanční prostředky využívány na spolupráci České republiky s mnoha předními mezinárodními organizacemi (např. EU, OSN) [13].

Pomoc ale nepřichází jen z kruhů státní správy, do mezinárodní humanitární pomoci se zapojuje také samospráva, nejčastěji kraje a města, částečně i obce. Je však vhodné upozornit, že finanční zdroje získané prostřednictvím státní správy nebývají přímo součástí vyhlášené veřejné sbírky [11].

Koordinace humanitárních týmů v zasažené oblasti

Koordinace humanitárních týmů, které působí v místech, kde se katastrofa udála, je velmi náročná z pohledu logistiky i času. Pokud v zasažené oblasti již nějaké mezinárodní organizace před náhlou událostí působily (příklad Haiti), akutní pomoc

může přijít rychleji, protože humanitární pracovníci jsou již na místě a mohou ihned zmapovat terén a určit konkrétní potřeby (co se týče materiální a pak zvláště i expertní pomoci). Proto jejich reálná přítomnost, ať už jsou na místě samém z jakéhokoliv důvodu, může de facto představovat „výhodu“ pro zasaženou zemi (či lokalitu). Poté humanitární pracovníci dané neziskové organizace vytvoří tým, kde má každý stanovenou oblast působnosti (někdo se stará o problematiku vody, jiný o zdravotní pomoc a mnohé další okruhy činností). Jednotliví zástupci těchto rozdělených sfér působnosti se společně schází na tzv. clusteru, o kterém již byla zmínka na straně [11].

Poskytování humanitární pomoci

Ministerstvo Vnitra ČR v průběhu realizace poskytování humanitární pomoci stále spolupracuje s Ministerstvem zahraničních věcí ČR, které zajišťuje např. komunikaci se zastupitelským úřadem, informace z postiženého státu, víza pro členy záchranné jednotky (dále jen "odřadu") nebo víza pro doprovod materiální humanitární pomoci. Dále Ministerstvo zahraničních věcí zajišťuje protokolární předání humanitární pomoci [14].

Financování humanitární pomoci

Státní humanitární pomoc ČR do zahraničí je realizována z finančních zdrojů alokovaných vládou na daný rok ve státním rozpočtu do účelově vázané rezervy na humanitární pomoc Všeobecné pokladní správy. Z této účelově vázané rezervy čerpá finanční prostředky Ministerstvo zahraničních věcí a pravidelně informuje vládu o jejich čerpání.

Formy pomoci poskytované do zahraničí

Charakter, rozsah a teritoriální vzdálenost jsou určující pro zvolenou formu případné pomoci do zahraničí:
Z obecného hlediska lze hovořit o následujících formách okamžité humanitární pomoci:

- záchranářskou,
- materiální,
- finanční,
- poradenskou,

- kombinovanou.

Záchranářská humanitární pomoc do zahraničí

V rámci záchranářské humanitární pomoci do zahraničí jsou připraveny speciální typy odřadů. Odřady jsou vždy složeny tak, aby odpovídaly potřebám v místě mimořádné události (požární odřad, povodňový odřad, USAR odřad,…). Členy odřadu jsou hlavně příslušníci HZS ČR a dále mohou být součástí odřadu také příslušníci kynologických brigád, specialisté Státního ústavu jaderné, chemické a biologické ochrany, Policie ČR, vojáci z povolání a ostatní složky IZS.

Materiální humanitární pomoc do zahraničí

Materiální humanitární pomoc do zahraničí je poskytována na základě konkrétní žádosti postiženého státu, která je následně českou stranou zvážena a humanitární pomoc je případně Českou republikou poskytnuta. O materiální humanitární pomoci také rozhoduje Ministerstvo vnitra v dohodě s Ministerstvem zahraničních věcí.

Finanční humanitární pomoc do zahraničí

O poskytnutí finanční humanitární pomoci do zahraničí rozhoduje Ministerstvo zahraničních věcí ČR ve spolupráci s MV - generálním ředitelstvím HZS ČR. Pomoc je většinou poskytována prostřednictvím mezinárodních organizací nebo přímo na bankovní konto určené postiženým státem.

Poradenská humanitární pomoc do zahraničí

V tomto případě vysílá Česká republika do postižené oblasti specialisty a odborníky nebo poskytuje potřebné informace směřující k zamezení ztrát na lidských životech nebo k omezení materiálních škod.

Kombinovaná humanitární pomoc do zahraničí

Při tomto druhu pomoci se kombinují předcházející čtyři formy pomoci.

Přeshraniční spolupráce

ČR má uzavřeny mezivládní dvoustranné dohody o spolupráci a pomoci při katastrofách, živelních pohromách a jiných mimořádných událostech se všemi sousedními zeměmi a s Maďarskem, což umožňuje záchranným jednotkám v případě mimořádné události překračovat státní hranici ve zjednodušeném režimu. V rámci přeshraniční spolupráce jednotky příslušného územního celku zasahují na území příslušného územního celku sousedního státu na základě uvedených dohod. Žádost o pomoc si předávají operační střediska příslušných územních celků, popř. operační středisko územního odboru. Uzavřené dohody dále upravují např. společná školení, cvičení, vzájemnou výměnu informací, používání radiostanic, náhrady vzniklých škod, použití letadel, atd. [14].

Zásady poskytování pomoci do zahraničí

Základním hlediskem je **celková efektivita a přínos poskytnuté pomoci**, tedy její potřebnost, rychlost, vhodný obsah v závislosti na potřebách postižené země, efektivita využití dostupných národních či mezinárodních zdrojů, přiměřenost disponibilních finančních a technických prostředků a personálních kapacit, teritoriálně politická kritéria (vyváženost, diplomatické souvislosti), využití mezinárodní koordinace pomoci a spolupráce s českými i mezinárodními nevládními organizacemi.

Rozhodujícím hlediskem pro poskytnutí pomoci Českou republikou musí být potřeby postižené země, vyjádřené oficiální žádostí příslušné vlády. Nabídka českých vládních či nevládních organizací, skupin nebo jednotlivců je druhořadá.

Při rozhodování o tom, zda a jakou formou pomoc poskytnout, je nutné mít na zřeteli **přiměřenost pomoci nejen potřebám postižené země, ale také ke skutečné výši rozpočtových prostředků na české straně** pro takové účely vyčleněné s ohledem na jejich nejefektivnější využití a konkrétní přínos. Teritoriální hledisko při poskytování pomoci do zahraničí je třeba posuzovat ve spojení s dalšími zahraničně politickými aspekty bilaterální či multilaterální povahy. Dalším aspektem vládní pomoci je také snaha o **zvýšení prestiže a mezinárodního kreditu České republiky v zahraničí**. Svou primární užitečností plní humanitární pomoc i významnou funkci i jako nástroj zahraniční politiky české vlády [14].

Časové hledisko a trvání pomoci

Česká republika respektuje mezinárodně uznávanou zásadu "kontinuity pomoci", jež představuje **provázaný a harmonizovaný sled akcí**, postupujících od neodkladné, okamžité pomoci v krizové situaci bezprostředního ohrožení, přes pomoc při obnově až po rozvojovou pomoc. Neexistuje všeobecná shoda o kritériích pro odlišení a definování jednotlivých etap (fází) pomoci, nicméně z časového hlediska rozlišujeme:

- **pomoc neodkladnou** - k záchraně životů a ochraně zdraví osob před následky mimořádné události, poskytnutou v průběhu několika hodin podle možností a schopností poskytovatele a na dobu několika dnů, maximálně týdnů,
- **pomoc při obnově** - při obnově základních podmínek života, hygieny, bydlení, poskytování stravy apod. v časovém horizontu několika týdnů až měsíců, v nejchudších oblastech světa může trvat i několik let,
- **pomoc rozvojovou** - touto formou se předkládaný materiál nezabývá, protože se jedná o pomoc specifickou nad rámec zákona č. 239/2000 Sb., o IZS [14].

Rozhodující faktory pro vyslání záchranné jednotky do zahraničí:

Vzdálenost a místo určení:

- **teritorium Evropy a ostatní státy světa**, které požádají o pomoc pro speciálně připravené a předurčené síly v podobě záchranné jednotky**,** vyslání se předpokládá pozemní cestou na vzdálenost do 1000 km (17 h) nebo letecky na vzdálenost nad 1000 km a do 2500 km,
- **sousední státy ČR-** pro předurčené síly hasičských záchranných sborů krajů**,** přeprava se předpokládá pozemní cestou (výjimečně v odůvodněných případech i letecky) [14].

Rozhodovací proces

Při zapojování ČR do mezinárodních záchranných operací nebo při poskytování humanitární pomoci do zahraničí je v souladu s existujícími předpisy uplatňován následující rozhodovací proces:

Prvotní informace

Ústřední správní úřady, zpravidla **Ministerstvo vnitra nebo Ministerstvo zahraničních věcí, obdrží informaci o závažné mimořádné události v zahraničí** (v souladu s mezinárodní smlouvou nebo mezinárodní úmluvou, od mezinárodní organizace (UN-OCHA, EU-MIC, NATO-EADRCC, IAEA ad.) nebo jiného zahraničního orgánu (např. zastupitelský úřad), ze sdělovacích prostředků, apod.), anebo obdrží přímo žádost o pomoc.

Vyhodnocení informací

Dostupné informace mezi sebou orgány státní správy konzultují a vyhodnocují je. **Hodnotí zároveň možnost, zda je ČR schopna poskytnout žádanou formu pomoci**. Informace o mimořádné události jsou konzultovány mezi Ministerstvem vnitra a Ministerstvem zahraničních věcí, případně s dalšími ministerstvy a ústředními správními úřady a technicky je připraven způsob poskytnutí pomoci, jsou informovány předurčené síly a prostředky.

Rozhodnutí

Po vyhodnocení situace a zjištění, že poskytnutí pomoci je vhodné a možné, jsou informováni ministři vnitra a zahraničních věcí a je po nich požadováno rozhodnutí. V případě požadavku na vyslání záchranářské nebo materiální pomoci ministr vnitra navrhne možné varianty, resp. komodity, které je ČR schopna poskytnout. Ministr zahraničních věcí rozhodne o uvolnění finančních prostředků.

Aktivace sil a prostředků

Po rozhodnutí o poskytnutí pomoci v určené finanční výši jsou **aktivovány předurčené síly a prostředky a probíhá svoz specialistů, příprava k vyslání materiální pomoci nebo záchranné jednotky,** je připravována dokumentace k vyslání pomoci, je ustanoven velitel jednotky, resp. konvoje, jsou vydány valutové prostředky a jsou stanoveny další podrobnosti. V zájmu urychlení této fáze tento proces probíhá podle předem připravených modelových postupů s nezbytnými odchylkami podle konkrétní situace [14].

Nejvíce kroků je třeba provádět v případě vysílání záchranné jednotky. Obecně se v takovém případě činnost pracovní skupiny štábu IZS připravující zapojení záchranné jednotky do mezinárodní záchranné operace soustřeďuje především na:

- Komunikaci s Ministerstvem zahraničních věcí, orgány postiženého státu, příslušnými zastupitelskými úřady a mezinárodními organizacemi,
- získávání aktuálních informací o situaci v místě předpokládaného nasazení jednotky a analýzu těchto informací,
- zajišťování splnění vízových, celních a dalších obdobných povinností,
- zajištění transportu jednotky,
- zajištění pojištění pro členy jednotky,
- zjišťování potřebných kontaktních informací,
- zajištění průjezdu či přeletu nad tranzitními zeměmi,
- zajištění přepravy z místa příletu do místa zásahu v postižené zemi,
- zajištění map postiženého území,
- vypracování příslušných dokumentů.

Realizace

Materiální pomoc nebo záchranná jednotka opouští stanoveným způsobem území státu a na místě se zapojuje do provádění záchranných prací, případně plnění dalších úkolů.

Právní úprava poskytování humanitární pomoci do zahraničí

Podle **§ 7 odst. 1 písm. b) zákona č. 239/2000 Sb.**, o integrovaném záchranném systému a o změně některých zákonů, ve znění pozdějších předpisů, Ministerstvo vnitra plní úkoly v oblasti zapojení České republiky do mezinárodních záchranných operací při mimořádných událostech v zahraničí a poskytování humanitární pomoci do zahraničí v součinnosti s Ministerstvem zahraničních věcí.

Na základě **§ 7 odst. 4 písm. a) zákona č. 239/2000 Sb.**, Ministerstvo vnitra organizuje záchranářskou a materiální pomoc do zahraničí ve spolupráci s Ministerstvem zahraničních věcí, složkami integrovaného záchranného systému nebo ústředními správními úřady. Podrobná pravidla stanoví prováděcí předpisy, především **nařízení vlády č. 463/2000 Sb.**, o stanovení pravidel zapojování do mezinárodních záchranných operací, poskytování a přijímání humanitární pomoci a náhrad výdajů vynakládaných

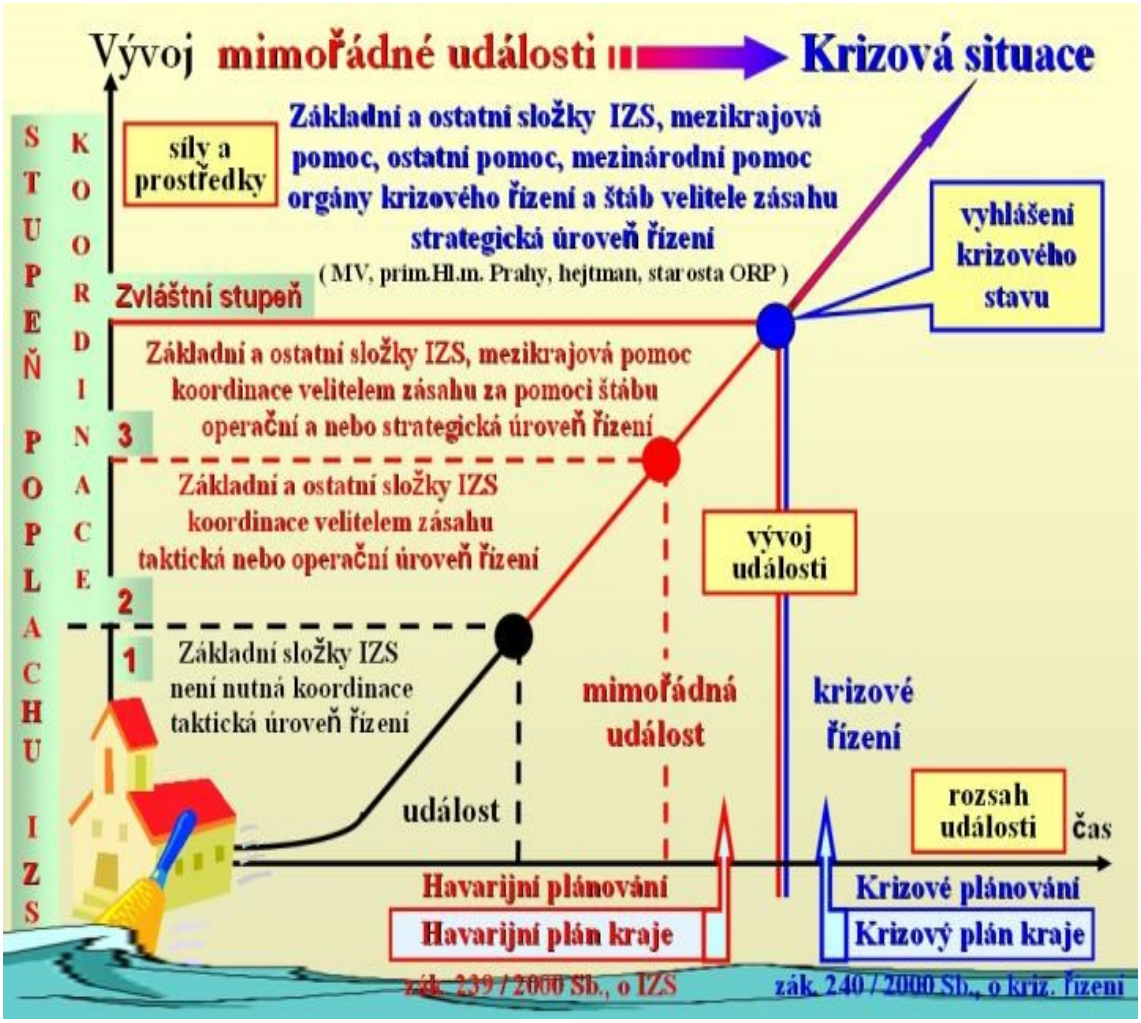
právnickými osobami a podnikajícími fyzickými osobami na ochranu obyvatelstva, ve znění **nařízení vlády č. 527/2002 Sb.**

Zákon č.151/2010 Sb., o zahraniční rozvojové spolupráci a humanitární pomoci poskytované do zahraničí a o změně souvisejících zákonů, upravuje rozhodovací pravomoci v otázkách poskytování humanitární pomoci.

Dalším důležitým právním předpisem je **zákon č. 133/1985 Sb.**, o požární ochraně, ve znění pozdějších předpisů, jenž umožňuje Ministerstvu vnitra ČR soustřeďovat a nasazovat síly a prostředky požární ochrany při poskytování mezistátní pomoci bez ohledu na to, kdo s nimi disponuje. Spolupráci Hasičského záchranného sboru ČR s mezinárodními organizacemi a zahraničními subjekty umožňuje **zákon č. 238/2000 Sb.**, o Hasičském záchranném sboru ČR, ve znění pozdějších předpisů. Hlavní zásady zapojování sil a prostředků České republiky do mezinárodních záchranných operací a poskytování humanitární pomoci do zahraničí byly popsány v materiálu Zapojení České republiky do mírových a záchranných operací a humanitární pomoci, který byl přijat **usnesením vlády ČR č. 458 ze dne 9. května 2001** [14].

Příloha č. 3 – Místo a úloha havarijního plánování v návaznosti na vývoj MU

Obr. Příloha 3.1 Místo a úloha havarijního plánování



Zdroj: [6]

Příloha č. 4- Charakteristika prvků dopravních systémů

Tabulka. Příloha 4.1 Charakteristika prvků dopravních systémů

Dopravní systémy	**Dopravní prostředky**	**Dopravní cesty, obslužné objekty**
Silniční	nákladní automobily, vozidla pro přepravu osob	silniční sítě, čerpací stanice, parkoviště, odstavné plochy, kamionové terminály, překladiště,…
Železniční	lokomotivy, tažené železniční vozy	železniční svršek, koleje, mosty, tunely, nádraží, železniční depa, překladiště
Říční	nákladní lodě, lodě pro přepravu osob	splavné říční toky, vodní kanály, vodní nádrže, jezera, přístavy, zdymadla,…
Námořní	různé typy nákladních a osobních lodí, kontejnerové lodě, tankery,…	mořské plochy, vymezené koridory pro lodní dopravu, přístavy, doky,…
Letecké	letadla pro osobní a kontejnerovou dopravu	vzdušný prostor s vymezenými koridory, letiště pro smíšenou nebo jen nákladní přepravu, hangáry,…
Potrubní	kompresní, čerpací stanice	sítě plynovodů, ropovodů, teplovodů
Lanové	kabiny pro dopravu osob, kontejnery pro dopravu rud zavěšené na nosném laně, pohyb většinou tažným lanem	lanové dráhy, stanice

Zdroj: [7]

Příloha č. 5 - Komunikační a informační technologie ve složkách IZS

Informační technologií je každý elektronický přístroj schopný zpracovávat nějaké informace (neboli provádět algoritmus), tedy přijmout nějaká vstupní data, samostatně s nimi provést nějaké operace a vydat příslušná data výstupní (popřípadě část této technologie). Obor informační technologie hledá nejefektivnější řešení, jak tyto technologie vytvořit, sestavit, propojit, zdokonalit, vynalézají nové a vytvářejí programy, které zajistí komunikaci s dalšími programy, které bude používat uživatel přístroje (aplikacemi nebo softwarem). Tolik informace z encyklopedie. Pro krizové řízení lze z toho vybrat zařízení využívaná ke sběru dat pro vyhlášení výstrah (elektronické odčty výše hladiny řek, monitorovací radiační síť, přístroje ke sledování síly zemětřesení a podobně), zařízení využívaná k varování a vyrozumění, řízení zásahu, zpracování relačních databází, využívání informačních systémů (mobilní telefony, radiové analogové a digitální sítě, počítačové sítě a počítače) [15].

Informační technologie IZS

U složek integrovaného záchranného systému lze počítat mezi informační technologie i zařízení sloužící k přenosu informací a dat jednak mezi pracovníky jednotlivých složek, spojení mezi jednotlivými jednotkami navzájem, spojení mezi základnou (případně KOPIS) a výjezdovou jednotkou, spojení mezi jednotlivými složkami IZS. Jde o koordinaci záchranných a likvidačních prací odehrávajících se na třech úrovních:

- **Taktická** – na místě zásahu, kde se mimořádná událost projevuje svými účinky, nebo kde se projevy mimořádné události předpokládají. Zde se provádějí záchranné a likvidační práce.
- **Operační** – tzv. úroveň operačních středisek základních složek IZS přičemž operační střediska Hasičského záchranného sboru jsou současně operačními středisky a informačními středisky IZS. Střediska jsou zřízena v krajích a na ministerstvu vnitra. Operační střediska zajišťují obsluhu linek tísňového volání (112, 150, 155, 158), a jsou pro každého občana místem, kde může přivolat pomoc v nouzi. Operační a informační středisko IZS má mezi ostatními operačními středisky koordinační roli. Může požadovat uveřejnění informací ve sdělovacích prostředcích, ovládá systémy varování a vyrozumění pro obyvatelstvo a je spojovým uzlem mezi místem zásahu a třetí řídící úrovní IZS.

Sem je také svedena tísňová linka 112 určená pro ohlášení jakékoliv tísně pro občany z cizích zemí. Operační a informační středisko IZS povolává na žádost velitelů zásahů k zásahům ostatní složky IZS podle poplachového plánu IZS. Tento plán také třídí mimořádné události podle rozsahu jejich následků do čtyř skupin (stupně poplachu). Prostřednictvím operačních a informačních středisek IZS také hejtman kraje a starosta obce s rozšířenou působností jsou při své koordinaci záchranných a likvidačních prací povinni předávat Ministerstvu vnitra zprávy o mimořádné události a jejich průběhu a vyžadují pomoc.

- **Strategická** – představuje přímé zapojení starosty obce s rozšířenou působností, hejtmana kraje nebo Ministerstva vnitra do koordinace záchranných a likvidačních prací. To nastává v situaci, kdy velitel zásahu o jejich koordinaci požádá a v případě hejtmana kraje a Ministerstva vnitra také, když je mimořádná událost ohodnocena nejvyšším stupněm poplachu dle poplachového plánu IZS. Ke svému rozhodování pak jako poradní orgán využívají krizové štáby zřízené podle zvláštního právního předpisu [15].

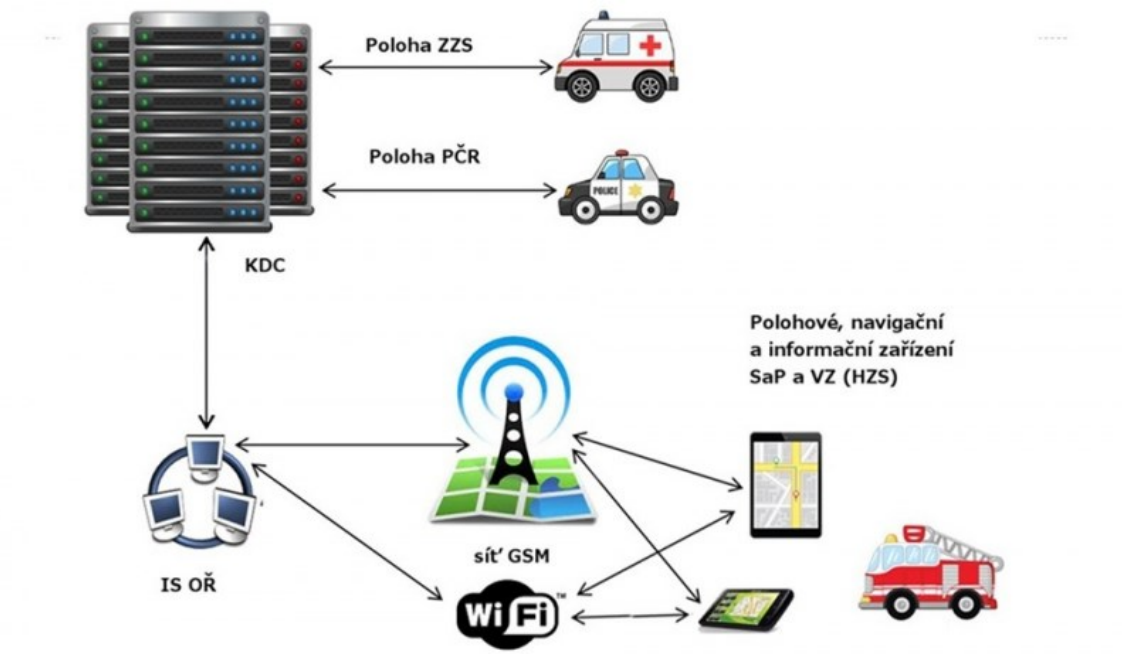
Komunikace složek IZS

Významným nástrojem při koordinaci IZS je jak ve fázi příprav na mimořádnou událost, tak i při provádění záchranných a likvidačních prací systém krizové komunikace. Krizovou komunikací je přenos informací mezi státními orgány, územními samosprávnými orgány a složkami IZS, za využití následujících prostředků hlasového i datového přenosu informací (viz také obrázek P5.1):

- účelové telekomunikační sítě Ministerstva vnitra, která zabezpečuje hlasovou a datovou komunikaci připojení hromadné radiokomunikační sítě IZS,
- hromadné radiokomunikační sítě IZS provozované ministerstvem pod názvem PEGAS, k běžnému provozu složek jako jediného radiokomunikačního prostředku se používá tam, kde byl ukončen přechod z radiokomunikačních technologií do hromadné sítě,
- veřejné pevné telekomunikační sítě, ve kterých je spojení jištěno v rámci regulačních opatření uplatněním přednostního spojení,
- veřejné mobilní telekomunikační sítě, ve kterých je spojení zajištěno v rámci regulačních opatření uplatněním přednostního spojení, tzv. krizové telefony,

- prostředky mobilní telekomunikační sítě vyčleněné k zajišťování spojení orgánů krizového řízení a obcí,
- záložní rádiové sítě v přímém režimu na určeném kmitočtu, případně v režimu umožňujícím propojení,
- spojek nebo vytvořené rádiové sítě pro tranzitní přenos zpráv, které se použijí při selhání všech technologií, nebo
- mobilní telekomunikační sítě a zařízení, jejichž nasazení může povolit velitel zásahu nebo územně příslušné operační a informační středisko IZS při nedostatečné kapacitě standardně používaných spojovacích prostředků, např. mobilní buňky operátorů pro lokální posílení kapacity mobilní sítě [16].

Obr. Příloha 5.1 Schéma datových přenosů vzhledem k silám a prostředkům IZS



Zdroj: [33]

Organizaci spojení pro zajištění vlastních činností složky IZS provádí každá složka samostatně. v této souvislosti je potřeba zmínit povinnost MV umožnit orgánům a složkám IZS krizovou komunikaci v účelové telekomunikační síti MV. Poskytovatelé služeb v oblasti komunikací jsou povinni spolupracovat s MV při přípravě a řešení způsobu krizové komunikace a jednotného evropského čísla tísňového volání 112. Podrobnosti o způsobu krizové komunikace a spojení v IZS a o strukturách sdílených

dat a způsobu využívání komunikačních sítí složkami IZS stanoví prováděcí předpis k zákonu o IZS.

Analogové rádiové spojení

Analogová rádiová síť Hasičského záchranného sboru ČR a součinnosti v IZS (dále jen „ARS“) je určena pro rádiové spojení jednotek Hasičského záchranného sboru ČR (dále jen „HZS ČR“) a pro součinnost s jednotkami požární ochrany (dále jen „jednotky PO“) ostatních zřizovatelů a součinnost s dalšími základními a ostatními složkami IZS (dále jen „další složky IZS“) [17].

Analogová radiová síť je tvořena rádiovými prostředky HZS ČR a rádiovými prostředky jednotek PO ostatních zřizovatelů a dalších složek v IZS při součinnosti je organizována jako stálá rádiová síť s nepřetržitým provozem řídící základnové radiostanice.

Analogová radiová síť ARS se používá zejména ke komunikaci mezi operačními středisky ke komunikaci mezi operačním střediskem a jednotkou PO, ke komunikaci na místě zásahu, k přenosu dat na vyhrazených kmitočtech, k vyhlašování poplachu jednotkám PO, ke svolání členů jednotek SDH obcí, k součinnostnímu spojení mezi jednotkami PO navzájem a mezi jednotkami PO a dalšími složkami IZS [17].

Telekomunikace – přenos informace v jakékoli podobě prostřednictvím drátových, rádiových, optických nebo jiných přenosových systémů radiokomunikace – druh telekomunikace přenášející informaci prostřednictvím rádiových vln.

Radiokomunikační prostředky jsou:

- radiostanice – stanice určené pro příjem a vysílání rádiových signálů v kmitočtovém pásmu k tomu účelu vyhrazeném,
- přenosná radiostanice – radiostanice napájená z vlastního akumulátoru vybavená vlastní anténou,
- mobilní radiostanice – radiostanice napájená palubním napětím instalovaná v mobilním dopravním prostředku, resp. mobilní požární technice, vybavená anténou instalovanou na karosérii,
- pohyblivá radiostanice – přenosná nebo mobilní radiostanice,
- základnová radiostanice – radiostanice se síťovým napáječem vybavená anténou instalovanou na objektu,
- dálkově ovládaná radiostanice – základnová radiostanice ovládaná pomocí linkové nebo rádiové komunikace,

- rádiový převáděč – základnová radiostanice pro zabezpečení semi - duplexního provozu [17].

Po roce 1989 se změnou politického systému se uvolnil trh, vzniklo mnoho firem, které se začaly zabývat dovozem a prodejem radiostanic. Nebylo třeba žádat o devizové prostředky a bylo možné nakupovat radiostanice od předních světových firem MAXON, MOTOROLA, BENDIX KING, ASCOM, MIDLANT (AEL) a dalších.

Digitální rádiové spojení

HZS ČR používá, s výjimkou HZS hl. m. Prahy, digitální radiokomunikační síť PEGAS od 1. 2. 2007 v úrovni komunikace mezi operačními středisky a vozidly. Na místě zásahu, kromě HZS Ústeckého, Moravskoslezského a Jihomoravského kraje, není digitální systém používán. Pro zajištění vzájemné radiokomunikace jsou však jednotky PO (minimálně velitelé družstev) vybaveni digitálními terminály. Jednotky sboru dobrovolných hasičů obcí používají analogovou rádiovou komunikaci, stejně, jako ostatní jednotky PO. V této části dokumentu jsou shrnuty požadavky dle priorit na digitální radiokomunikační technologii z pohledu HZS ČR [17].

Radiová síť PEGAS (dříve kvůli existenci názvu GSM sítě Pegas nepoužívané jméno) je v ČR budována od roku 1994, kdy byla na základě výběrového řízení Ministerstva vnitra ČR vybrána digitální technologie TETRAPOL od francouzského výrobce Matra (nyní EADS). Tato technologie byla v tehdejší době jedinou digitální rádiovou technologií na světě a společnost již měla za sebou několik instalací funkčních sítí. Technologie se začala v ČR budovat v projektu s názvem PEGAS, jehož jméno je nyní používáno jako označení sítě. Digitální technologie umožňuje již nyní mnoho služeb, včetně již v systému zavedené šifry, čímž je systém použitelný rovněž pro bezpečnostní složky. Nabízí rovněž služby obvyklé v digitálních systémech GSM (SMS, identifikace volajícího, apod.) a současně respektuje charakter práce a činností složek IZS, kterým je dispečerské řízení provozu. Hlavním cílem budování tohoto systému je usnadnit všem složkám IZS jejich činnost na místě zásahu a současně zabezpečit tolik požadovanou možnost vzájemné komunikace. Toto se týká celé České republiky a tak mohou záchranáři s pomocí této sítě bez problémů komunikovat na jakémkoli jejím místě [17].

Požadavky na radiokomunikační systém je možné spatřit z několika pohledových úhlů. Jedním je pohled z hlediska komunikačně-organizačních vrstev (strategická/taktická/operační) a druhým pohled na systém jako celek z technického

pohledu a vztahu k zajištění dostupnosti služeb. Průnikem obou úhlů je možné definovat požadavky na systém, které budou pro HZS ČR výchozím předpokladem pro rozvoj v oblasti radiokomunikace. V definici tzv. „nulového stavu“, tedy stavu, ze kterého bude systém PEGAS dále rozvíjen, spatřuje HZS ČR i další možnosti, směrem k jasné a zřejmé definici požadavků na související systémy a projekty (např. standardizace operačních středisek IZS nebo úprava stávajících, na síť PEGAS navázaných, koncových dispečerských zařízení) [17].

Za společenskou objednávku ze strany uživatelů je možné považovat souhrn bodů, které se týkají jak technologických, tak organizačních změn. Za zásadní je nutné považovat v oblasti technologie:

- spolehlivost infrastruktury - úprava topologie a redundance k eliminaci domino efektů při degradaci dostupnosti služeb (například vlivem povětrnostních vlivů),
- kapacita souběžných komunikací tak, aby byly naplněny základní požadavky na provoz systému pro IZS,
- pokrytí území rádiovým signálem, aby byly splněny požadavky všech základních složek IZS,
- datový portál a poskytování služby AVL, které je nezbytné pro stanovení základní úrovně poskytování služeb směrem k projektu jednotné úrovně operačních středisek a rozvoji v oblasti výkonu služby.

V oblasti organizace je nezbytné rozhodnutí, jaké parametry budou v následujícím období dodržovány a sledovány a jakým způsobem bude zajištěn servis, ve prospěch složek IZS.

Systém PEGAS v současném období poskytuje útvarům PČR dostatečné možnosti spojení při rutinních i mimořádných činnostech. Policie ČR, která systém využívá od počátku výstavby, má pro své potřeby dostatečné počty skupinových komunikací. Snahou je maximální využití jak hlasových, tak v posledním období i datových služeb. Docílení spokojenosti však není automatické, nýbrž je podmíněno nepřetržitou prací spojařů s uživateli a sledováním a vyhodnocováním provozních dat. Nutností je okamžitá reakce na nedostatečnou znalost uživatele, vadné baterie, informace o výpadku infrastruktury, příprava plánu spojení a další činnosti. v případě úplného začlenění dalších bezpečnostních složek státu, jako Celní správa či Vězeňské služby do organizační struktury PEGAS, by tak umožňovalo v rámci plnění některých úkolů, například při transportech vězňů, či spolupráci na dálniční síti, zabavování padělků

z tržnic a dalších akcích. Rovněž dovybavení pracovníků zdravotní záchranné služby v rámci celé ČR by při mnoha společných akcích bylo přínosem [17].

Krizové telefonní spojení

Počínaje rokem 2002 mají k dispozici vedoucí ústředních orgánů státní správy, členové bezpečnostních rad a krizových štábů, vedoucí a vybraní pracovníci složek IZS, hejtmanů a starostové obcí k dispozici tzv. „mobilní krizové telefony“ včetně služeb s tím spojených. Krizový telefon má zpravidla dvě čísla. Na jednom z nich, tzv. krizovém je kromě celé škály služeb operátora, pro účastníka zejména zajištěno:

- předem zvolená priorita, tedy přednost volání v rámci provozované sítě,
- provoz mobilního telefonu i při omezení ostatních účastníků sítě při jejím přetížení,
- přenos datových informací,
- informační systém založený na informačním web serveru.

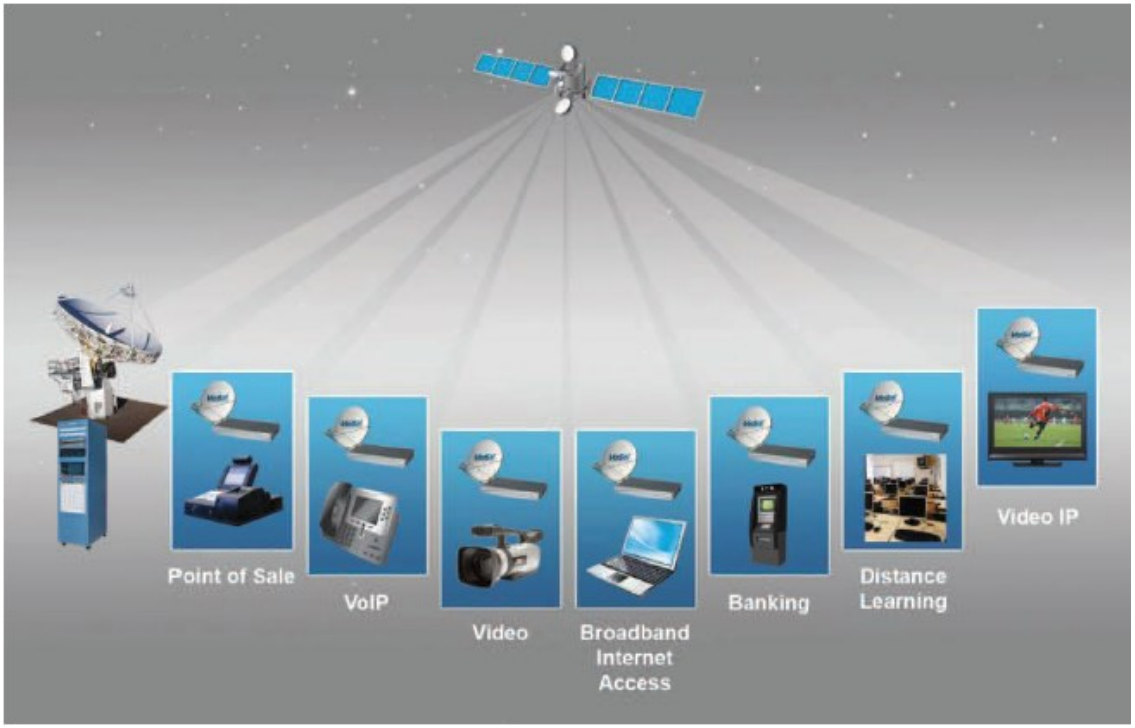
Krizové telefony zavedlo MV na základě rozhodnutí vlády. Celkový počet krizových mobilních telefonů dosáhl v ČR počtu téměř 19000 ks. Nespornou výhodou telefonů je unifikace mobilního telefonu a všech příslušenství telefonu. To má řadu provozních výhod. v době vyhlášení krizového stavu je provoz na těchto telefonech pro účastníky zdarma [16].

Satelitní spojení

V náročném prostředí oblasti elektronických komunikací se v krizových situacích můžeme orientovat také na satelitní služby, které mají stále nezastupitelnou úlohu při zajišťování spojení a distribuci signálu. Satelitní služby se uplatňují zejména v náročných podmínkách, kde svou flexibilitou umožní zajistit rychle spojení podle specifických požadavků prostředí a to i v případě mimořádných událostí. Výhodou satelitních komunikací je především jejich nezávislost na jakékoli pozemní infrastruktuře. Vedle speciálních spojů, provozovaných pro konektivitu účastníků na sítě po celém světě, lze užít satelitních systémů pro přístup k internetu odkudkoliv. Představuje to mimo jiné i spolupráci se zahraničními partnery, kteří provozují rozsáhlé satelitní sítě nejen s celoevropskou působností. Tyto služby lze doplnit vlastními řešeními, které vycházejí z nových možností technologií "minihubů", efektivně

využívajících satelitní pásmo s dynamickým řízením provozu [18]. Na obrázku č. P5.2 můžeme vidět různé využití satelitních služeb.

Obr. Příloha 5.2 Služby poskytované satelitním komunikačním systémem



Zdroj: [34]

VTC

Videokonference jsou často chápány, jako nákladná řešení zaměřená na top management. Vzhledem k ceně a kvalitě jednotlivých řešení je v dnešní době videokonference dostupná pro každého**.** Právě nákladná profesionální řešení jsou mnohdy brzdou pokroku, protože brání využití v běžném pracovním kontaktu. Instalace a zavedení současných řešení pro videokonference je často záležitost několika hodin nebo dnů.

Videokonference prostřednictvím webové kamery poskytuje výrazné zlepšení komunikace oproti telekonferenci nebo chatování, kdy může docházet k pocitům odcizení kvůli velké vzdálenosti nebo nemožnosti vnímat neverbální projevy ostatních stran.

Videokonference jednoho člověka s více lidmi – jeden účastník hovoří nebo prezentuje, ostatní pasivně přijímají a mohou reagovat pouze hlasově. Každá osoba může být připojena z libovolného místa na světě. Tento způsob je výborný například pro školení

na dálku**,** kdy všichni získají příležitost sledovat jednotlivé činnosti školitele a mohou se ho dotazovat. v případě propojení se sdílenou plochou je to nejefektivnější způsob práce a komunikace online.

Videokonference více lidí navzájem – všichni účastníci se vidí navzájem prostřednictví malých oken na obrazovce monitoru nebo projektoru. Pro celkový dojem nebo lepší zobrazení si lze každého účastníka zvětšit na plnou obrazovku [15].

Možnosti využití videokonference:

- strategická rozhodování,
- týmové porady oddělení a reporting,
- přednášky a semináře,
- řešení krizové situace,
- operativní schůzky.

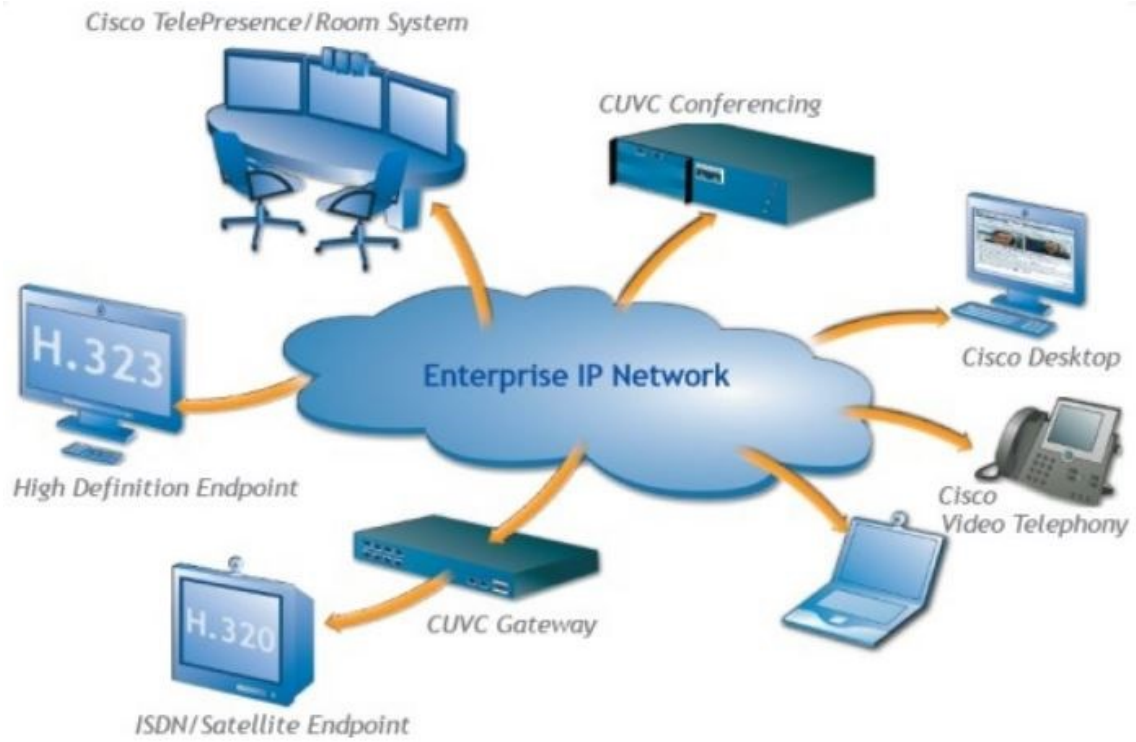
Co je potřeba pro videokonference:

- Webová kamera, sluchátka a mikrofon – nezbytný základ pro videokonference. Nové notebooky mají často tyto komponenty zabudované. Je to velice úsporné řešení, které vás nenutí nosit sebou další vybavení.
- Dostatečně výkonný počítač nebo jiný hardware - videokonference je náročnější na hardware, tedy na výkon počítače, než telekonference a narůstá s počtem účastníků.
- Kvalitně zvolený software - řada programů má různé nároky na zatížení počítače i náročnost na rychlost připojení k Internetu. Např. program Skype patří z hlediska telekonference (pro dvě osoby) do té horší – méně kvalitní skupiny. Neúměrně zatěžuje počítač a na slabších počítačích dochází k přerušování obrazu. Naproti tomu existuje software, který nemusíte instalovat, a váš počítač zatěžuje jen minimálně.

Výhoda videokonference spočívá v tom, že máme dostupné obrázky a informace v reálném čase z místa mimořádné události a krizový management může na základě těchto údajů provádět účelnější rozhodnutí v řešení dané MÚ nebo KS, včetně sledování dopadu při realizaci těchto opatření.

Nejnověji ověřené použití informačních systémů z místa přírodní katastrofy v Japonsku zaznamenalo použití sociálních sítí, jako je např. Facebook a Twitter [15].
Obrázek č. P5.3 ukazuje, jakými způsoby lze přenést telekonferenční hovor.

Obr. Příloha 5.3 Možné způsoby přenosu telekonferenčního hovoru



Zdroj: [35]

Využití sociálních sítí jako komunikační infrastruktury

Facebook je rozsáhlý společenský webový systém sloužící hlavně k tvorbě sociálních sítí, komunikaci mezi uživateli, sdílení multimediálních dat, udržování vztahů a zábavě. Se svými 2 miliardami aktivních uživatelů (červen 2015) je jednou z největších společenských sítí na světě. Facebook je určen pro sdílení videa mezi přáteli. Jedno video může mít maximálně 1024 MB a může být maximálně 20 minut dlouhé. Videa se dají jednoduše prohlížet pomocí technologie Flash a podobně jako v aplikaci Fotografie zde můžete označovat svoje přátele [19].
Twitter již od svého počátku fungoval na principu krátkých zpráv do délky 140 znaků, které ale velmi často obsahovaly zkrácený odkaz na webovou stránku, o které chtěl autor něco sdělit. Během fungování Twitteru se rozšířily určité výrazy, které s ním jsou neoddělitelně spjaty, jako je „tweetnout“ (zveřejnit vzkaz na Twitteru). Přestože na

českém internetu nemůže Twitter soutěžit s Facebookem co do počtu uživatelů, díky slušné informační hodnotě většiny příspěvků se stal pro mnoho lidí zdrojem informací dodávaných takřka v reálném čase [19].

Facebook a další sociální sítě se staly nedílnou součástí online životů velkého množství uživatelů, stejně jako jim podobné služby. Do této kategorie spadá také Twitter, v jehož rámci si může kdokoliv, kdykoliv a kdekoliv „tweetnout“ své aktuální pocity, postřehy či zážitky. Facebook nebo Twitter,jsou v dnešním moderním světě naprostým fenoménem. V extrémních případech by se dalo říci, že kdo není na sociální síti, jako by nebyl. Právě tato masovost užívání nejmodernějších informačních systémů nám dává možnost dostat se i na místa“ kde se zrovna něco děje“ a využívat těchto zpráv, které bychom jinak nezískali, i v oblasti krizového řízení [15].

Hromadné informační prostředky

Součástí opatření IZS je i potřeba uveřejnit tísňové informace potřebné pro záchranné a likvidační práce. v této souvislosti je uložena povinnost všem, kdo provozují hromadné informační prostředky, včetně televizního a rozhlasového vysílání. Tyto subjekty jsou povinné uveřejnit tísňové informace potřebné pro záchranné a likvidační práce na základě žádosti operačního a informačního střediska IZS neprodleně a bez úpravy obsahu a smyslu, navíc bez náhrady nákladů s tím spojených.

Vybavení IZS počítačovou technologií

Velký rozmach v používání výpočetní techniky u Hasičského záchranného sboru se dostavil v začátku 90. let. Souviselo to s vývojem nových počítačů a růstem výroby a snížením ceny. Tím dochází k masovějšímu používání této moderní techniky. V dnešní době počítače bereme jako normální součást života a neumíme si ho už bez ní ani představit. U HZS bylo zřízeno i nové oddělení ASŘ - automatizace systému řízení a následně i oddělení informatiky. Tato oddělení se zabývají zpracováním rozšiřujícího se informačního toku do podoby umožňujícím vybavování potřebných informací v reálném čase [15].

Příloha č. 6 – Zabezpečení utajení a kryptografie

Neutajovaná část komunikačního centra

Směrem od neutajovaného WAN routeru do vnitřní části neutajované sítě je komunikace vedena přes softwarovou dvojici firewallů, doplněná bezpečnostními prvky IDS a IPS (detekce a prevence proti určitým bezpečnostním hrozbám a útokům). Za touto bezpečnostní zdí, která filtruje bezpečný provoz, se nachází CORE DISTRIBUTION SWITCH obsahující 2 a více vysokokapacitních distribučních MLS switchů *(multi - layerswitch)*. Tyto switche jsou propojeny do mesh topologie tak, aby vytvořily co nejefektivnější přenos dat mezi jednotlivými lokálními středisky a podpořily svou kapacitou rychlé a spolehlivé spojení směrem ven k NU WAN ROUTERU. Blok MLS switchů můžeme v této práci nazvat „Distribučním blokem“. Na tento blok jsou napojené veškeré zařízení pro poskytování všech komunikačních, informačních a řídících služeb. Tedy jak služby pro mailovou komunikaci, DHCP, DNS, Antivirové ochrany, správy pro aktualizace všech systémů, autorizace, tak i služeb VoIP, VTC a správy sítě.

Od tohoto bloku jsou vedeny veškerá spojení kabelem k jednotlivým neutajovaným lokálním střediskům. Tyto střediska jsou složeny ze switche a NU LAN routeru. Tyto síťové prvky slouží k připojení jednotlivých uživatelů. Znázorněná střediska jsou oddělená a každé má svou dedikovanou velikost sítě dle požadovaných prostředků. Uživatelské prostředí obsahuje koncové prostředky uživatele, jako jsou počítače, VoIP telefony, VTC vybavení pro přenos videa a zvuku atd.

Utajovaná část komunikačního centra

Jelikož tato část je citlivá pro přenos neveřejných informací, bylo třeba myslet na to, že musí být dodrženy co nejvyšší bezpečnostní standarty pro komunikaci, mezi vnitřní, utajovanou části, směrem přes satelit do ostatních komunikačních uzlů. Tato bezpečnost je zaručena pomocí fyzických šifrovacích zařízení, které zakódují veškerá data do neutajované části pomocí 2048 bitového kódu. Na NU WAN ROUTER je napojen hlavní UTWAN ROUTER, který přenáší utajovaná data do a ven z uzlu pomocí zabezpečených tunelů. Směrem od UTWAN ROUTERU do vnitřní části neutajované sítě je komunikace vedena přes dvojici softwarových firewallů, doplněná bezpečnostními prvky IDS a IPS (detekce a prevence proti určitým bezpečnostním

hrozbám a útokům). Komunikace je pak směrována přes „Distribuční blok“ přímo na rádio-reléový anténní spoj, který zprostředkovává veškerou komunikaci mezi lokálními uzly, které byly z hlediska náročnosti na výstavbu spojeny rádiovým zabezpečeným přenosem.

Tyto střediska můžou obsahovat utajované i neutajované lokální části. „Distribuční blok“ je podle toho rozděluje na vstupním portu a přenáší dál do jednotlivých částí podle tohoto kritéria. Utajované pak míří přímo na vnitřní kryptografické zařízení u UT-WAN routeru.

KC vyšších úrovní jsou složeny z NU-LAN ROUTERU, Distribučního bloku a UT-LAN ROUTERU, popř. Utajovaného Distribučního bloku. Všechny vyjmenované síťové prvky slouží k připojení jednotlivých uživatelů. Jednotlivá centra jsou oddělena a každé má svou dedikovanou velikost sítě dle požadovaných prostředků. Uživatelské prostředí obsahuje koncové prostředky uživatele, např. PC, VOSIP telefony, VTC vybavení pro přenos videa a zvuku atd.

K oddělení utajované komunikace již dochází před UT-LAN ROUTEREM, před kterým je umístěno, vnitřní krypto zařízení, které ve VPN (virtuální síti) přeposílá data na vnitřní krypto zařízení zapojené u UT-WAN ROUTERU. Jednotlivá lokální střediska je možné ještě spojovat mezi sebou dalšími bezdrátovými (wifi) zařízeními pro lepší vnitřní komunikaci a vytvářet tak i redundantní okruhy.

Autor (vypracoval)	Bc. Vladimír Hubáček
Název DP	Zabezpečení služeb uživatelů komunikačního uzlu
Studijní obor	Logistika
Rok obhajoby BP	2019
Počet stran	108
Počet příloh	6
Vedoucí BP	Oldřich Kodym
Oponent BP	
Anotace	Komunikace je nezbytnou součástí post krizových logistických procesů a komunikační uzel vhodně zasazený do struktury záchranných prvků je předpokladem k zefektivnění komunikace krizových štábů na všech úrovních a záchranných sborů, které s plným nasazením bojují o záchranu lidských životů, zdraví a majetku. Pomocí komunikačního uzlu je možné zvýšit informovanost nejen záchranných týmů, ale také civilního obyvatelstva v poškozené oblasti.
Klíčová slova	Krize, Post krizové procesy, Komunikační uzel, Network, Komunikační infrastruktury, Informační služby, Komunikační služby
Místo uložení	ITC (knihovna) Vysoké školy logistiky v Přerově
Signatura	