VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ

ÚSTAV MANAGEMENTU

FACULTY OF BUSINESS AND MANAGEMENT

DEPARTMENT OF MANAGEMENT

MOŽNOSTI PROVOZOVÁNÍ BEZPEČNÉHO INFORMAČNÍHO SYSTÉMU HZS JMK

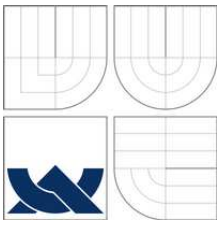
DIPLOMOVÁ PRÁCE

MASTER´S THESIS

AUTOR PRÁCE Bc. HANA SEČKAŘOVÁ

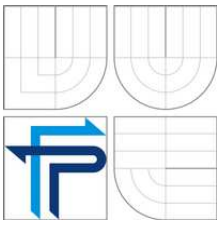
AUTHOR

BRNO 2013



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA PODNIKATELSKÁ

ÚSTAV MANAGEMENTU

FACULTY OF BUSINESS AND MANAGEMENT

DEPARTMENT OF MANAGEMENT

MOŽNOSTI PROVOZOVÁNÍ BEZPEČNÉHO INFORMAČNÍHO SYSTÉMU HZS JMK

HOW TO GET A SECURE INFORMATION SYSTEM HZS JMK

DIPLOMOVÁ PRÁCE

MASTER´S THESIS

AUTOR PRÁCE — Bc. HANA SEČKAŘOVÁ

AUTHOR

VEDOUCÍ PRÁCE — prof. Ing. JIŘÍ DVOŘÁK, DrSc.

SUPERVISOR

BRNO 2013

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2012/2013
Ústav managementu

ZADÁNÍ DIPLOMOVÉ PRÁCE

Sečkařová Hana, Bc.

Řízení a ekonomika podniku (6208T097)

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách, Studijním a zkušebním řádem VUT v Brně a Směrnicí děkana pro realizaci bakalářských a magisterských studijních programů zadává diplomovou práci s názvem:

Možnosti provozování bezpečného informačního systému HZS JMK

v anglickém jazyce:

How to Get a Secure Information System HZS JMK

Pokyny pro vypracování:

Úvod
Vymezení problému
Cíle práce
Teoretická východiska práce
Současná situace
Analýza problému
Vlastní návrhy řešení
Závěr
Seznam použitých informačních zdrojů
Seznam zkratek a pojmů
Seznam obrázků a tabulek
Rejstřík
Přílohy

Seznam odborné literatury:

BASL,J. a R.BLATNÍČEK.Podnikové informační systémy:
Podnik v informační společnosti.2.vyd.Praha:Grada Publishing,2000.283s.ISBN
978-80-247-2279-5.
MOLNÁR,Z.Efektivnost informačních systémů.1.vyd.Praha:Grada Publishing,2000.144s.ISBN
80-7169-410-X.
RYBIČKA,J.Informatika pro ekonomy.4.vyd.KONVOJ Brno,2008.147 s.ISBN
978-80-7302-150-4.
ŘEPA,V.Analýza a návrh informačních systémů.1.vyd.Praha: EKOPRESS,2000.185s.ISBN
80-86119-13-0.

Vedoucí diplomové práce: prof. Ing. Jiří Dvořák, DrSc.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2012/2013.

L.S.

prof. Ing. Vojtěch Koráb, Dr., MBA	doc. Ing. et Ing. Stanislav Škapa, Ph.D.
Ředitel ústavu	Děkan fakulty

V Brně, dne 22.05.2013

Abstrakt:

Diplomová práce se zabývá návrhem modelu pro bezpečné provozování informačního systému (IS) na úrovni manažerského řízení u Hasičského záchranného sboru (HZS) Jihomoravského kraje (JMK).

Součástí diplomové práce jsou analýzy současného stavu informačního systému HZS a posouzení jeho bezpečnosti a efektivnosti. Na základě těchto analýz jsou navrhnuty řešení pro zlepšen stávajícího stavu IS.

Klíčová slova:

Informační systém, integrace, bezpečnost, analýza

Abstract:

This master´s thesis contains the concept model for the safe operation of the information system (IS) at the level of management control in Fire and Rescue Brigade (HZS) Southern Region (JMK).

Part of this master´s thesis is analyse of current of an information systém in Fire and Rescue Brigade and evaluation of its security and effectiveness. A set of improvement propositions of the current state of information system was created based on those analyses.

Key words:

Information system, integration, security, analysis

Bibliografická citace práce:

SEČKAŘOVÁ, H. *Možnosti provozování bezpečného informačního systému HZS JMK*. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2013. 79 s. Vedoucí diplomové práce prof. Ing. Jiří Dvořák, DrSc.

Čestné prohlášení

Prohlašuji, že předložená diplomová práce je původní a zpracovala jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušila autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 21. ledna 2013

Podpis

Poděkování

Ráda bych poděkovala vedoucímu práce panu prof. Ing. Jiřímu Dvořákovi, DrSc. za cenné rady, připomínky a za ochotu mi poradit a pomoci s každým problémem vyskytující se během psaní mé práce.

Dále bych chtěla poděkovat KOPIS JMK a KŘ HZS JMK za věnovaný čas a cenné informace a připomínky potřebné k zpracování této práce.

OBSAH

1. Úvod

Diplomová práce se zabývá zhodnocením bezpečnosti informačního systému (dále jen IS) Hasičského záchranného sboru Jihomoravského kraje (dále jen HZS JMK) a následné návrhy na další opatření proti zneužití důvěrných dat.

Na informační systémy veřejné správy jsou kladeny vysoké požadavky, jelikož skrývají mnohdy utajená data určená pouze pro interní zpracování.

V dnešní době je každý podnik vystaven hrozbám zneužití dat z IS a především pokud se jedná o velmi citlivá a utajená data jako v případě veřejné správy. Tyto hrozby nemusí být pouze cílené ze strany útočníka, který chce získaná data zneužít, ale mohou vzniknout nahodile a proti některým se nelze důsledně bránit.

Jsou však opatření, která mohou hrozby ze zneužití dat z IS snížit. Pro správné posouzení se provádí analýza IS a vhodná bezpečnostní opatření, která z manažerského hlediska posoudím jako možné hrozby pro podnikový IS na základě provedené analýzy bezpečnosti.

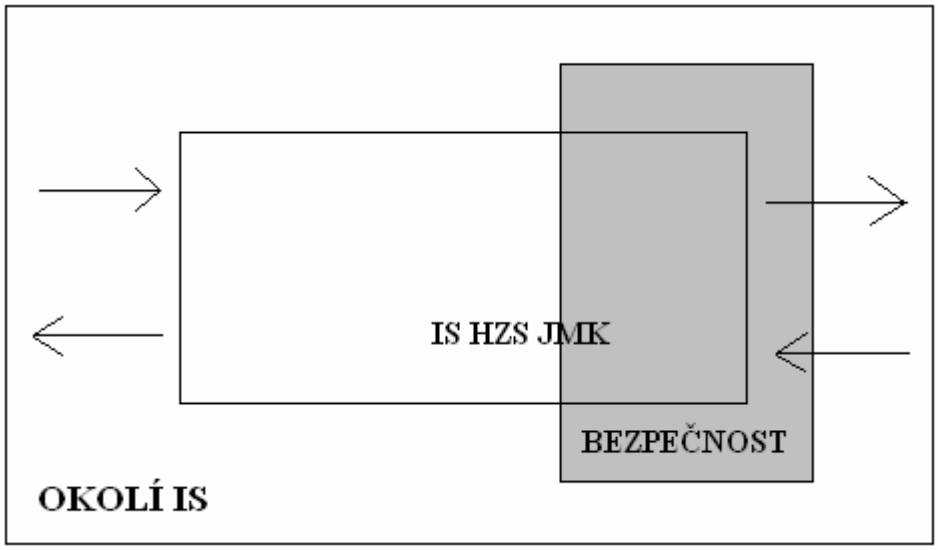
Tato práce se zabývá návrhem změn pro bezpečnostní politiku a efektivnější využití dat v IS HZS JMK. Obsahuje analýzu současného stavu IS v podniku a potřebné návrhy na změny v bezpečnosti IS proti zneužití dat.

2. Systémové vymezení problému

Účelem této práce je analyzovat současnou situaci IS HZS JMK a uživatelských práv, celková struktura systému a úroveň bezpečnosti IS. Jakým způsobem jsou uživatelská práva přidělena a jak jsou zabezpečeny různé formy omezení uživatelských práv.

Dále také i zjištění zabezpečení IS pro vstup jak z vnitřní sítě tak i z vnější sítě a to jak autorizovanými uživateli tak i uživateli s pokusem o nabourání se do systému se záměrem zneužití dat.

Na základě zjištěných poznatků nalézt nedostatky a navrhnout zlepšení stávající situace v rámci technického zpracování a omezit tak přístupu do systému nepovolaným osobám.



Obrázek 1: IS
Zdroj: Vlastní

3. Cíl práce

Cílem práce je, na základě analýzy informačního systému (IS) Hasičského záchranného sboru (HZS) Jihomoravského kraje (JMK), vytvořit model pro bezpečné provozování uvedeného IS na úrovni manažerského řízení.

V práci bude řešena analýza současného stavu z hlediska provázanosti IS v rámci používaných programů u TCTV a KOPIS *(viz. kap. 5)*, SWOT analýza současného stavu IS *(viz. kap. 5.12.)* a posouzení bezpečnosti IS pomocí analýzy bezpečnostních rizik *(viz. kap. 6)*.

Provedené analýzy budou podkladem pro návrhy na zlepšení stávající situace v informačním systému HZS a jejich zhodnocení z hlediska celkových přínosů pro podnik a ekonomická zhodnocení.

4. Teoretická východiska práce

„Informační systémy jsou speciálním typem systémů. Jedná se o komplex informací, informačních technologií, lidí, technických prostředků a metod sloužících ke sběru dat, přenosu, uchování a zpracování dat za účelem tvorby a prezentace informací. S rozvojem informačních a technologických procesů se podstatně změnila dimenze používání dat a informací. Do systémů začínají vstupovat znalosti, které mění možnosti jejich využití.“ [15]

Podniky usilují o získání integrovaného, plně automatizovaného řídícího systému, který by sloužil vedení podniků na všech úrovních řízení a ve všech oblastech činností. Takový systém se obecně nazývá jako podnikový informační systém a stává se neoddělitelnou součástí podnikového majetku.

Dochází k výraznému zkvalitňování ve využití informačních systémů a odpovídajících informačních technologií. Nová technika a technologie zpracování dat vyžadují nový přístup k organizaci práce a nové znalosti. Výsledkem je větší zapojení uživatele do procesu automatizace zpracování dat pro potřeby systému řízení. Efektivnější a kvalitnější zpracování dat zkracuje dobu odezvy požadavků za jednotku času, a tím poskytuje lepší podmínky pro rozhodovací, řídicí a kontrolní proces. Informační hodnota dat má velkou vypovídací schopnost ve vztahu chování k danému systému.[11]

4.1. Zavádění informačního systému

Implementace informačního systému je důležitou etapou při zavádění IS v podniku. Je-li nutné změnit stávající informační systém nebo jen nahradit část systému novým, je potřeba zvolit tu nejvhodnější variantu podle aktuální situace. Lze rozlišit několik různých možností při implementaci informačního systému, přičemž má každá určité výhody a nevýhody *(viz. kap. 7. 2).* [5]

Souběžná strategie

„Při souběžné strategii pokračuje činnost starého systému spolu se systémem novým po dobu několika pracovních cyklů (několik týdnů, či měsíců), a to tak dlouho, dokud nový systém nepracuje spolehlivě a starý systém může být proto opuštěn.“ [9]

Strategie je velmi bezpečná ale pro uživatele náročná, jelikož musí pracovat v obou systémech.

Pilotní strategie

„Při pilotní strategii se zavede nový systém např. v jednom oddělení, pobočce, či kanceláři a teprve po jeho ověření se zavede nový systém naráz v celé organizaci.“ [9]

Strategie je relativně bezpečná, ale náročná na kompatibilitu, úplnost dat a správné propojení obou systémů.

Postupná strategie

„Postupnou strategii použijeme především u rozsáhlejších systémů se složitými vzájemnými vazbami. Obyčejně začínáme úlohami, které jsou podmiňující pro ostatní úlohy a postupujeme v zavádění v souhlase s životním cyklem výrobku, či služby.“ [9]

Strategie je bezpečná, ale velmi časově náročná.

Nárazová strategie

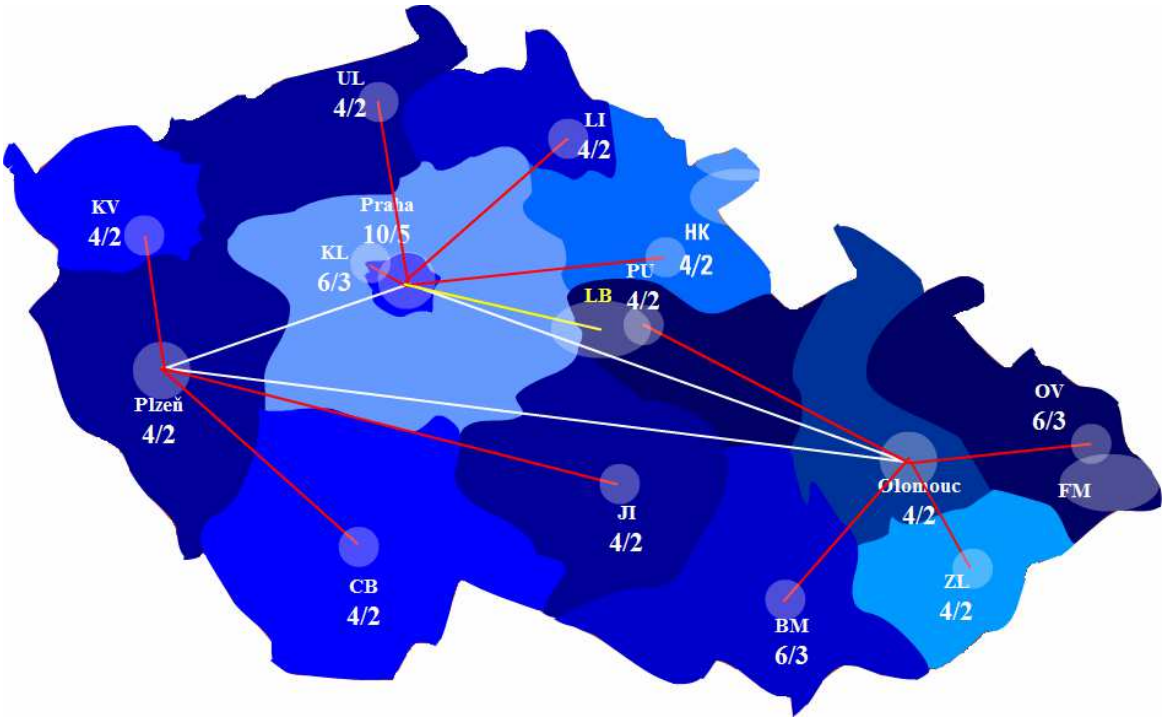
„Při nárazové strategii ukončíme činnost starého informačního systému a po nezbytně nutné pauze spustíme nový informační systém.“ [9]

Velmi riskantní řešení, ale rychlé a účinné.

4.2. Integrace systému TCTV 112 v ČR

„Povinnost zavést jednotné evropské telefonní číslo tísňového volání byla uložena všem členským státům s tím, že do konce roku 1996 musí být ve všech státech plně funkční. Pro přístup k tomuto tísňovému volání bylo stanoveno telefonní číslo **112**.“ [19]

Výhoda propojenosti systému u tísňového volání 112 je ve chvíli, kdy nastane krizová situace (např. povodně, vichřice) a konkrétní TCTV nestíhá přijímat a vyřizovat všechny hovory, pak jiná TCTV mohou tísňové volání převzít, vyhodnotit a získat potřebné informace *(Viz. obr. 1).* Po získání nutných informací zapíše operátor událost do systému a TCTV pro kterou je událost určena, si vše může v systému přečíst a poté předat událost dále operačnímu důstojníkovi dle místa určení aby mohl vyslat jednotky požární ochrany (JPO) k zásahu.[13]

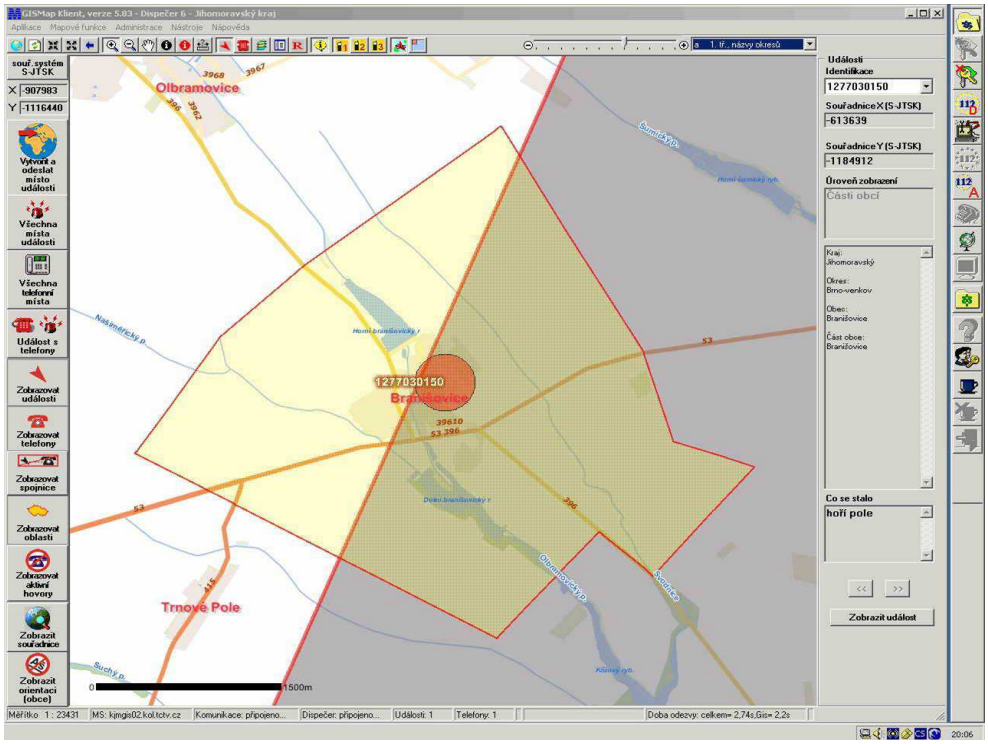


Obrázek 2: Propojenost TCTV 112 v ČR
Zdroj: [26]

4.3. Lokalizace místa

V rámci získání informací je také dostupná celorepubliková služba lokalizace místa, ze kterého je daný hovor uskutečněn. Tato informace je možná jak u mobilních telefonů tak i u pevných linek či telefonních budek.

V systému se objeví při volání telefonní číslo a případně i druh operátora. Pokud je to mobilní telefon, na mapě v systému se zobrazí přibližná lokalizace místa (u každého operátora je přesnost a styl zobrazení odlišná), pokud je to naopak pevná linka, je u zobrazeného čísla uvedena i adresa *(viz obr. 2).* U telefonních budek je bohužel někdy problém s přesným určením adresy, jelikož některé telefonní budky nemají uvedenou reálnou adresu místa kde stojí, ale adresu majitele, který danou telefonní budku provozuje, což může být někdy v rámci lokalizace matoucí. [13]



Obrázek 3: Lokalizace místa
Zdroj [26]

4.4. Systém HZS v Evropě

- ***Finsko***

Na základě zákona, přijatý v roce 2004, bylo zřízeno na území Finska 22 regionů s regionálními záchrannými středisky.

Požární jednotky lze rozdělit do čtyř skupin:

- Profesionální;
- Poloprofesionální;
- Dobrovolné;
- Závodní.

[6,7,8]

- ***Francie***

Zřizovateli požárníků jsou kraje. Všechny obce v rámci kraje má na starost jedno záchranné centrum, které má za úkol analýzu rizik, přípravu prostředků a koordinace činností požárníků. Činnosti jsou prováděny pomocí operativního střediska kraje. V Paříži a Marseille mají požárníci zvláštní status a jsou přímo podřízeni úřadům těchto měst.

Celkový stav požárníků je asi 250tis. osob a dělí se na:

- Dobrovolníky;
- Profesionály;
- Vojenské osoby.

[6,7,8]

➢ *Itálie*

Většina záchranných subjektů v rámci systému ochrany obyvatelstva je profesionální. Itálie je jednou z mála zemí západní Evropy, kde jsou požárníci převážně zaměstnanci státu v služebním poměru(obdobně jako v České republice). Téměř 90 %.

Rozdělení Národního požárního sboru je:

- Profesionálové;
- Vojáci prezenční služby,sloužící jako požárníci;
- Neorganizovaní dobrovolníci.

[6,7,8]

➢ *Německo*

Dle současné legislativy jsou požárníci v Německu z převážné většiny obecním zařízením a zařízením zejména velkých průmyslových subjektů. Většina požárních sil je tvořena dobrovolníky. Profesionálové jsou zastoupeni ve 100 největších městech.

S celkovým počtem asi 34,7 tis. požárních stanic je zabezpečeno celoplošné pokrytí území Německa v 10 minutových dojezdových časech od ohlášení.

Cekem je v Německu asi 1,3 mil. požárníků a dělí se na:

- Z povolání;
- Dobrovolné;
- Podnikové;
- Mladí požárníci.

[6,7,8]

➢ *Polsko*

Základem Celostátního záchranného a protipožárového systému představuje Státní požární ochrana. Jedná se převážně o státní službu v rámci služebního poměru a v menší míře o civilní zaměstnance.

Většina polských dobrovolných požárníků je sdružena ve Svazu dobrovolných požárníků (dále jen Svaz), který je celostátním samosprávným spolkem. (který je spolkem celostátní samosprávy).

- Aktivní příslušníci v rámci Celostátního záchranného a požárního systému;
- Sdružení mládežnických požárních družstev – asi 11 tis.

[6,7,8]

➢ *Rakousko*

V požární ochraně jsou téměř výhradně dobrovolníci – více než 95%. Jen v největších městech (Vídeň, Linec, Salcburk, Innsbruck, Štýrský Hradec a Klagenfurt) a v největších průmyslových podnicích jsou profesionálové.

Celkem je v Rakousku asi 320 tis. požárníků. A to:

- Z povolání;
- Dobrovolní;
- Podnikoví požárníci;
- Mladí požárníci.

[6,7,8]

➢ *Slovensko*

V požárních a záchranných složkách v rámci Hasičského a záchranného sboru se jedná o státní službu v rámci služebního poměru podle zákona č. 312/2001 o státní službě, dále o veřejnou službu podle zákona č.313/2001 o veřejné službě.

Celkový model Hasičských a záchranných sborů je obdobná jako v České republice. [6,7,8]

➢ *Slovinsko*

Nejdůležitější veřejná záchranná služba je požární služba, jejíž činnost se opírá především o dobrovolné požárníky.

Celkem je na území Slovinska asi 120 tis. požárníků,kteří se dělí na:

- Dobrovolné;
- Veřejno-právní;
- Podnikové.

Z celkového počtu organizovaných požárníků ve Slovinsku je asi 44 tis. aktivních členů, zařazených do služeb, z nichž tvoří naprostou většinu (mimo podnikových) dobrovolníci. [6,7,8]

➢ *Švýcarsko*

V rámci požární ochrany ve Švýcarsku patří nevládní organizace Švýcarský požární svaz. Kompetence vůči požárníkům mají kantony (územněsprávní jednotka ve Švýcarsku) včetně jejich povolávání k výkonu služební povinnosti.

Z hlediska charakteru výkonu služby se jedná o model kombinovaný s převahou povinné miliční služby dle zákona (místní požární sbory) a menším podílem profesionálů (požární stanice, podnikové a letištní sbory).

V současné době je ve Švýcarsku včetně Lichtenštejnského knížectví asi 120 tis. požárníků, které se člení na:

- Místní;
- Podnikoví;
- Příslušníci požárních stanic;
- Příslušníci letištních sborů.

[6,7,8]

➢ *Velká Británie*

Dle zákona jsou požárnici ve Velké Británii organizováni do Požární a záchranné služby (veřejní požárníci).

V rámci samosprávy existují v souladu se zákonem tři typy úřadů Požární a záchranné služby:

- Úřad protipožární a civilní ochrany – působí v metropolitních hrabstvích, v Londýně pod názvem Úřad protipožární ochrany a nouzového plánování;
- Kombinovaný úřad protipožární ochrany – tzv. All Purpose, vytvořený v rámci jedné nebo více obcí pro jejich území;
- Úřad protipožární ochrany území – zřizovatelem je samosprávné území s názvem podle toho, ve které historické zemi se nachází a s předurčením pro toto území.

[6,7,8]

5. Současný stav řešené problematiky

V analýze současného stavu je řešena provázanost informačního systému a bezpečnostní politiky IS v rámci HZS JMK a problematika různorodosti používaných aplikací v rámci IS HZS JMK.

Veškeré pohotovostní výjezdy jsou úzce provázány s informačním systémem HZS. Na základě správného vyhodnocení a rychlého předání informací pomocí provázanosti systému je možné co v nejkratší době zareagovat na události.

Celý informační systém HZS pracuje pod databázovým systémem Oracle, který je provázaný s dalšími aplikacemi potřebnými k fungování IS HZS. [1)]

5.1. Program IKIS I.

Aplikace na principu webového rozhraní odkazující se na databázový systém Oracle.

- Přehled událostí (zobrazení aktuální běžící rozpracované události nebo přehled událostí v určitém časovém rozmezí);
- Strážní kniha;
- JPO (specifické označení jednotky, název jednotky, seznam hlavní techniky a seznam pomocné techniky dané stanice);
- Kontakty. [13]

[1)] Na základě vlastního průzkumu a konzultací na KOPIS HSZ JMK a Krajském ředitelství HZS JMK.

5.2. Program IKIS II.

Souhrn aplikačních programů odkazující se na databázový systém Oracle a skládá se z určitých modulů:

- Strojní služba (auta, žebříky, plošiny atd.);
- Chemická služba (dýchací přístroje, ochranné obleky, teploměry .atd.);
- Technická služba (hadice, nafukovací vaky, hydraulické „nůžky“ atd.);
- Spojová služba (seznam a typy radiostanic – Matra, Motorola);
- Automatické akce (automatické spouštění sirén, světel, otevírání garážových vrat atd.);
- Administrace (přidělení práv osobám k nastavení přístupu do IS HZS).

Každá položka v databázi má své specifické označení aby nedocházelo k duplicitním hodnotám.[13]

5.3. Aplikace ISV Admin

Administrátorská aplikace databázového systému HZS „běžící“ pod Oracle. Aktualizaci a správnost dat zajišťuje IT administrátor na krajském ředitelství HZS JMK. [13]

5.4. Program SSU

Statistické sledování události - aplikace na obdobném principu jak IKIS II. s celkovým přehledem událostí v rámci JMK v různých fázích zpracování zásahů.

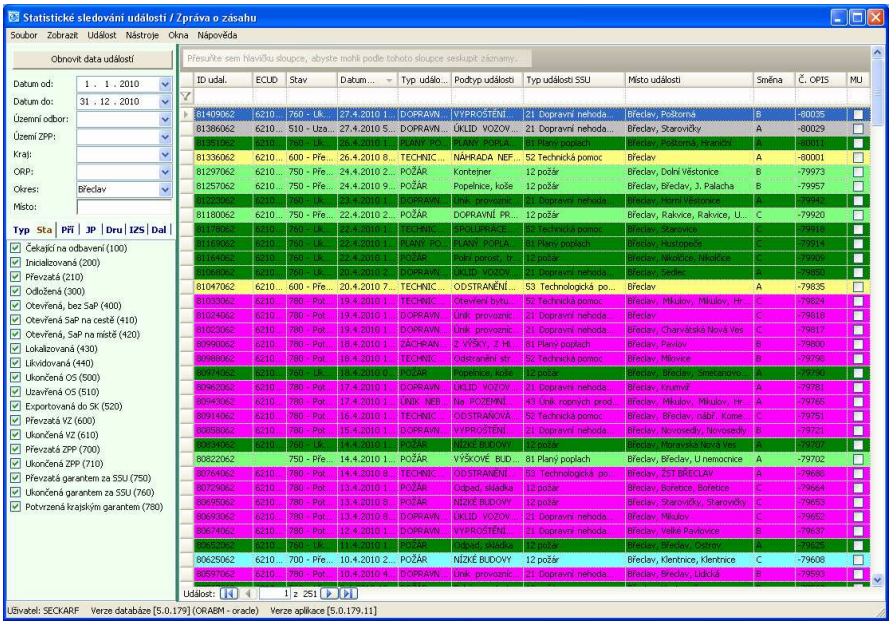
Celkové zobrazení je jen v rámci JMK ale na konci měsíce jsou data souhrnně odesílána na GŘ HZS ČR na centrální zpracování pro celou ČR *(viz. příloha 2)*.

Výstupem SSU je Zpráva o zásahu (ZOZ). [13]

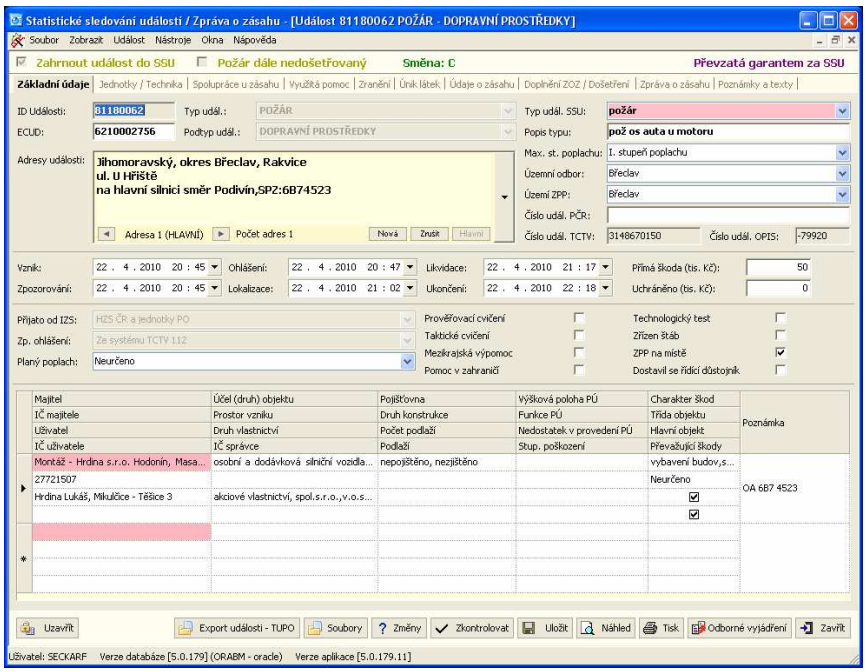
Vyplněnou ZOZ uloží velitel zásahu do systému jako uzavřenou událost a ta poté slouží ke kontrole o zásahu. Po vyplnění a uzavření ZOZ v systému se dále statisticky sleduje a zpracovává pro statistické sledování událostí (SSU).

Zde se dají sledovat a vyhodnocovat veškeré údaje k vytvoření statistickým podkladům. Např. počet nehod v kraji, počet pohotovostních výjezdů na stanici a na směnu, požáry v kraji, sledování rozsahu událostí, atd.

Na konci měsíce se veškeré statisticky zpracované ZOZ souhrnně odesílají na GŘ HZS ČR na centrální zpracování pro celou ČR. [13]



Obrázek 4: Seznam událostí v SSU
Zdroj:[25]

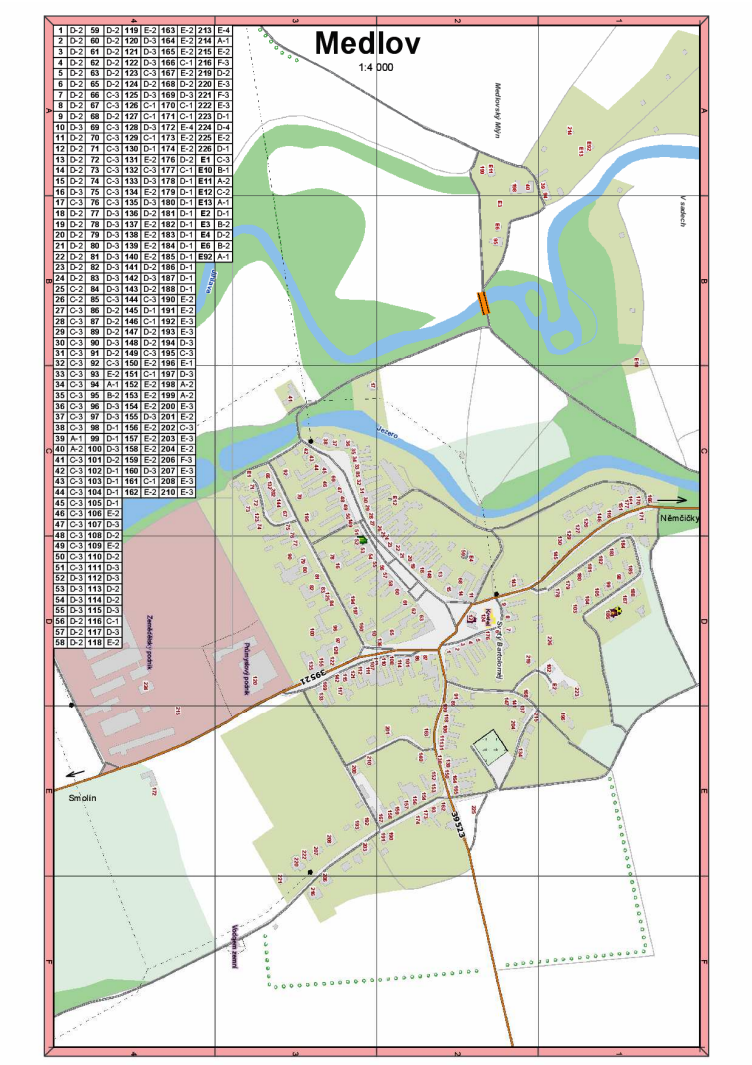


Obrázek 5: Náhled na událost v SSU
Zdroj: [25]

5.5. Vyhodnocení tísňového volání na TCTV

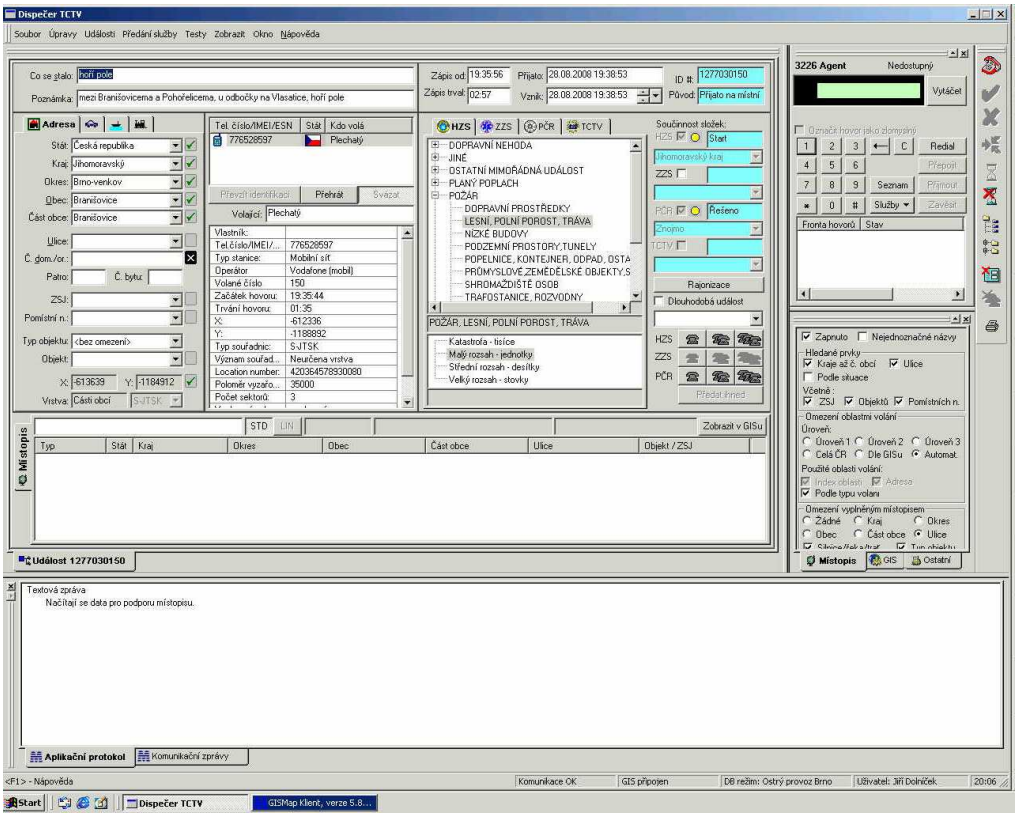
Vyhodnocení tísňového volání probíhá na základě informací podaných od volaného a následné určení místa díky speciálnímu programu Dispečer TCTV, do kterého danou událost zapisují operátoři tísňové linky 112 *(viz. obr. 6)*.

Při zadávání adresy nebo souřadnic se díky programu na další obrazovce zobrazí v grafickém zpracování (plán města) místo události, kterou mají k dispozici i JPO a díky ní se mohou lépe orientovat na místo události. Díky přepracovaným orientačním bodům s popiskami souřadnic je orientace rychlejší, což je při pohotovostním výjezdu důležité *(viz. obr. 5)*.



Obrázek 6: Plán města
Zdroj: [25]

Dále se automaticky v programu zobrazí veškeré informace o volajícím, jako např. číslo volajícího, typ stanice, operátor, začátek a délka hovoru, souřadnice z místa volání (*viz. kapitola 4.2.*), aj. [13]



Obrázek 7: Okno v programu Dispečer TCTV
Zdroj: [26]

5.6. Spojař

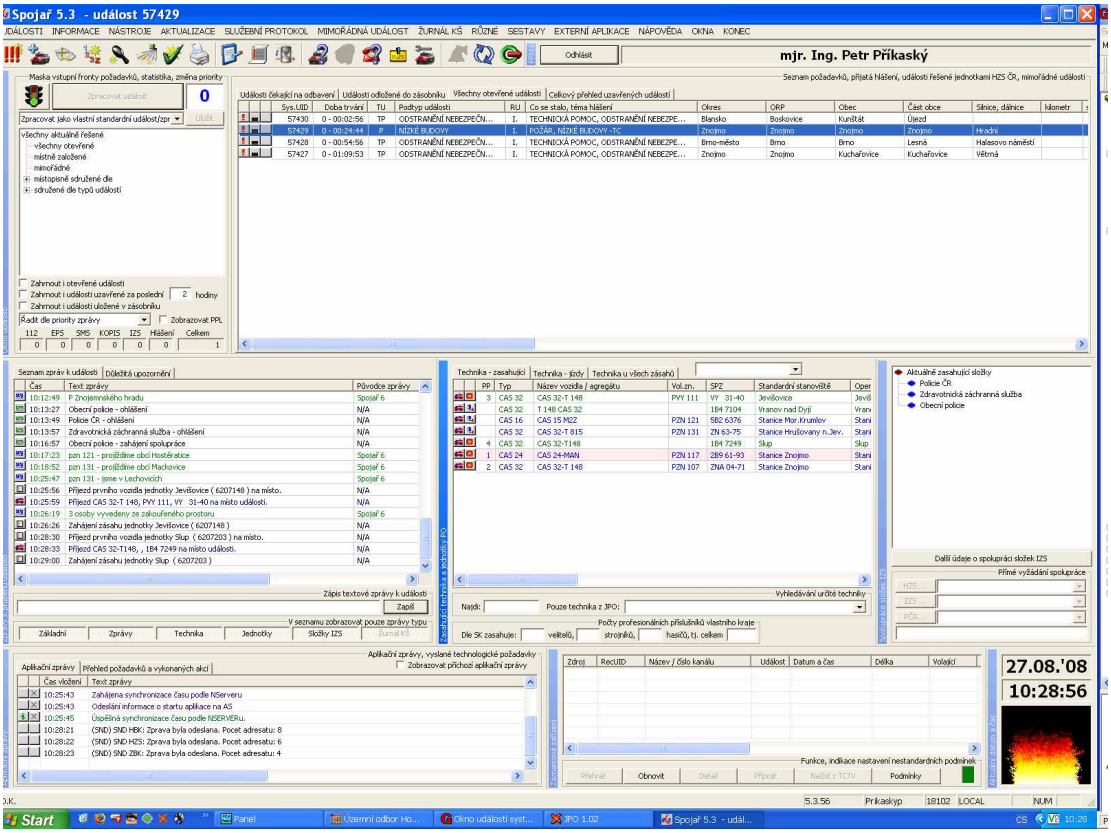
Program Spojař je vytvořen speciálně na zakázku pouze pro užívání HZS ČR. V programu se prolínají veškeré aplikace a programy odkazující se na databázový systém Oracle (*viz. IKIS I. ,IKIS II., ISV Admin, SSU*).

Programy a aplikace jsou mezi sebou provázané pomocí specifických označení a přesného přiřazení. Od veškeré techniky nacházející se na každé hasičské stanici až po přesné přiřazení osob na konkrétní stanici.

Program je nastaven, aby při různých výběrech stupňů požárních poplachů také přesně dodržoval stanovené vyhlášky a zákony, které určují jaká technika a kolik sil má k jistému zásahu vyjet.

Spojař slouží k detailnímu rozboru informací o zásahu a veškerých aut, techniky, pomocné techniky a osob vyjíždějící k zásahu *(viz. obr. 7)*.

Po vyplnění všech kroků (typ události, rozsah události, počet potřebných sil k zásahu, adresa události, potřebná technika), se souhrnně v systému zobrazí všechny vybrané jednotky operačním důstojníkem v poli výsledné množiny navržené techniky, typový návrh techniky k dané události. Tohle vyhledávání na konkrétní techniku či vozidlo se dá dohledat i pomocí programu IKIS II. (*viz. 5.2.)*. [13]



Obrázek 8: Okno událostí v programu Spojař
Zdroj:[25]

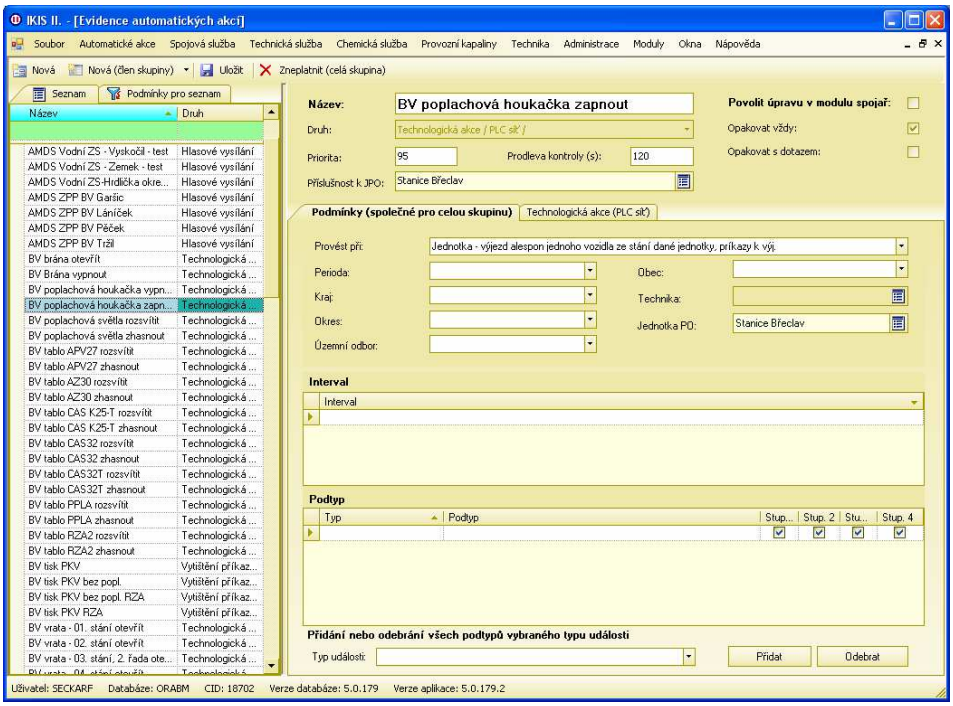
5.7. Provázání IS s technikou

Pokud jsou vyplněny všechny potřebné informace a vybrané jednotky se zobrazí správně, pak může operační důstojník zvolit „Výjezd s vyhlášením poplachu“ nebo „Výjezd bez vyhlášení poplachu“. Ve většině případů to je však „Výjezd s vyhlášením poplachu“ *(viz. obr. 9)*.

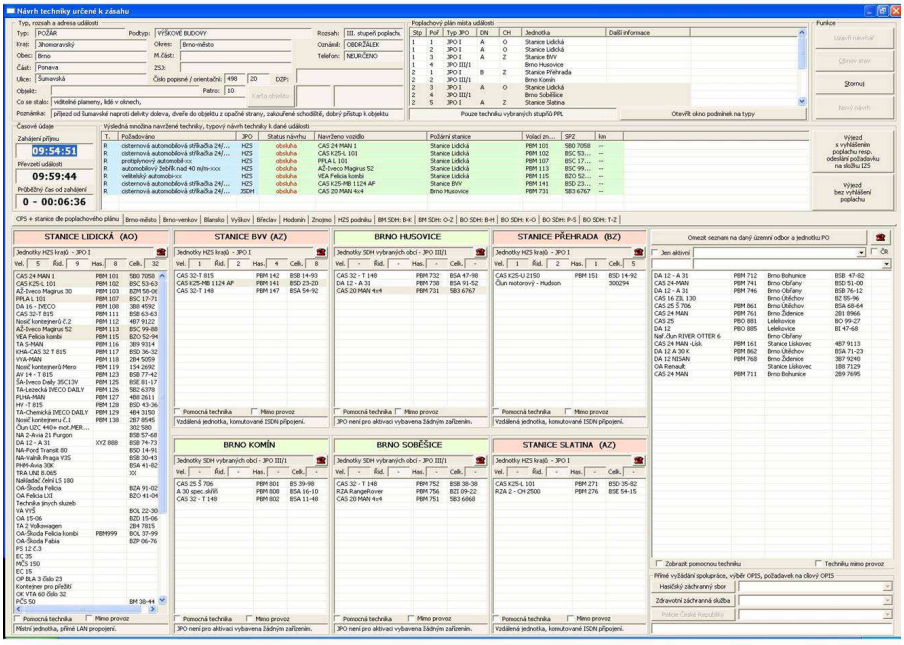
Díky provázanému IS se automaticky při vyhlášení poplachu provedou potřebné akce, které s souvisí s výjezdem jednotky.

Zahrnuje to např. spuštění poplachové houkačky *(viz. obr. 8)*, spuštění ohlášení informací o zásahu pomocí TTS (rozhlasové reproduktory, které danou událost hlasově oznámí na hasičské stanici pro výjezdové jednotky), tisk PKV, otevření vrat u příslušného auta, které bude vyjíždět k zásahu, při vyhlášení

poplachu rozesílání informativních sms o události pro výjezdové hasiče a zaměstnance HZS, kteří jsou zadaní v databázi pro zasílání těchto zpráv, aj. [13]



Obrázek 9: Automatické akce v IKIS II. – spuštění houkačky
Zdroj: [25]



Obrázek 10: Okno Návrhu techniky určené k zásahu
Zdroj: [25]

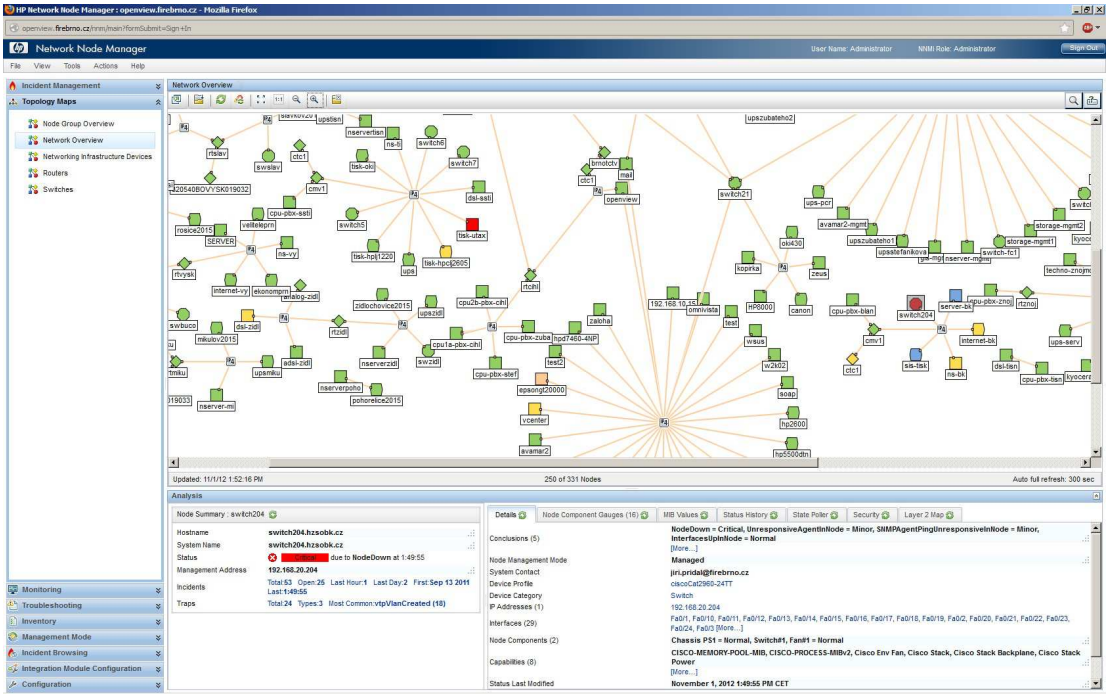
5.8. Program HP OpenView Network Node Manager

Network Node Manager (NNM) je aplikace z produktů HP OpenView společnosti Hewlett Packard**.** Je určená pro správu a management sítí. Je nejčastěji používaným produktem HP OpenView.

Poskytuje správcům informace o funkčnosti a efektivitě síťových prvků. NNM dokáže průběžně monitorovat stav spravovaných prvků a díky přesné a rychlé lokalizaci vzniklého problému tak přispívá efektivně k jeho následnému včasnému vyřešení *(viz. obr. 10)*.

- **Základní vlastnosti:**

- Automatické prozkoumávání a mapování celé sítové infrastruktury;
- Upozornění na změny či problémy, které se ve spravovaném IT prostředí vyskytnou;
- Propojenost událostí, identifikace prvotních příčin;
- Dlouhá řada podporovaných protokolů a podporovaných zařízení;
- Vytváření reportů z nasbíraných dat;
- Možnost grafických výstupů;
- Spolupráce s Domain Name systémy;
- Nástroje k testování dostupnosti stanic (Traceroute, Ping);
- Možnost nastavení prahových hodnot a definice událostí při jejich překročení. [16]



Obrázek 11: Okno v programu HP OpenView Network Node Manager
Zdroj: [25]

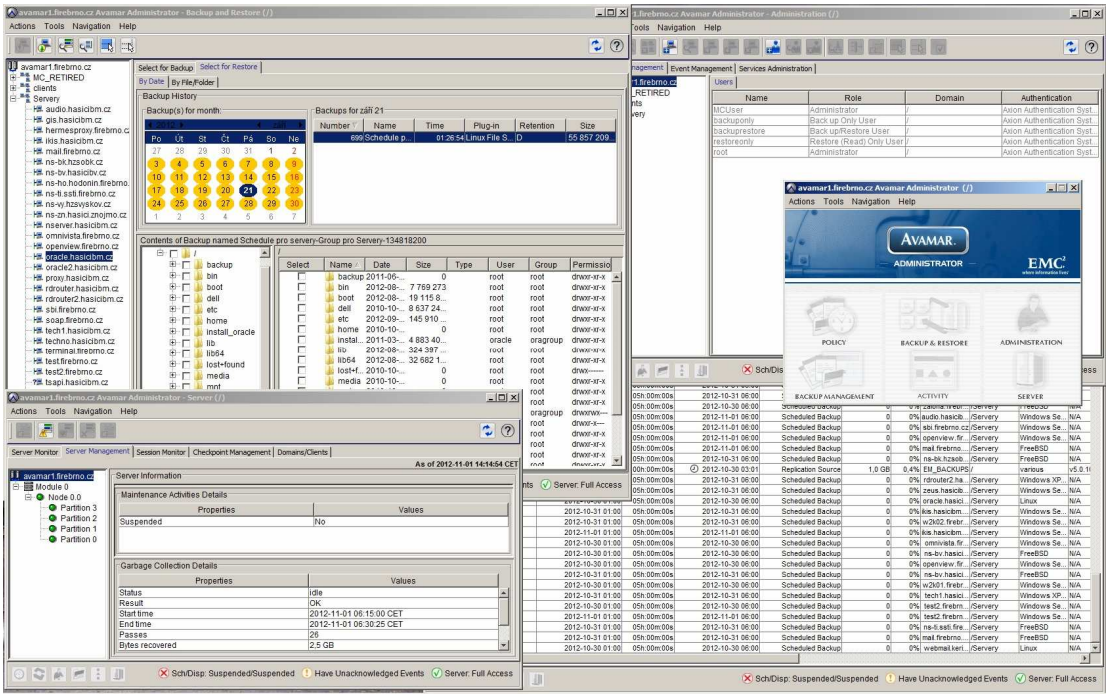
Dle funkčnosti zařízení rozlišujeme 3 barevná oznámení:

- **zelená :** plně funkční zařízení;
- **žlutá** : drobné závady zařízení;
- **červená :** kritický stav – nefunkčnost zařízení.

5.9. Program EMC Avamar

EMC Avamar umožňuje rychlé a efektivní zálohování a obnovení snížením velikosti zálohovaných dat, která jsou přenášena přes síť a ukládána. Avamar využívá deduplikaci dat, čímž snižuje zatížení sítě a zajišťuje úsporu místa na úložišti *(viz. obr. 11)*.

Deduplikace je speciální technika komprese dat, která zabraňuje ukládání stejných datových bloků na jednom úložišti. Deduplikační jednotka ukládá referenční informace o datové struktuře a díky tomu je schopná při zpětném čtení deduplikovaných dat zpět obnovit původní, komplexní informaci. Účelem deduplikace je úspora místa na datovém úložišti, v průměru o 92%. [14]



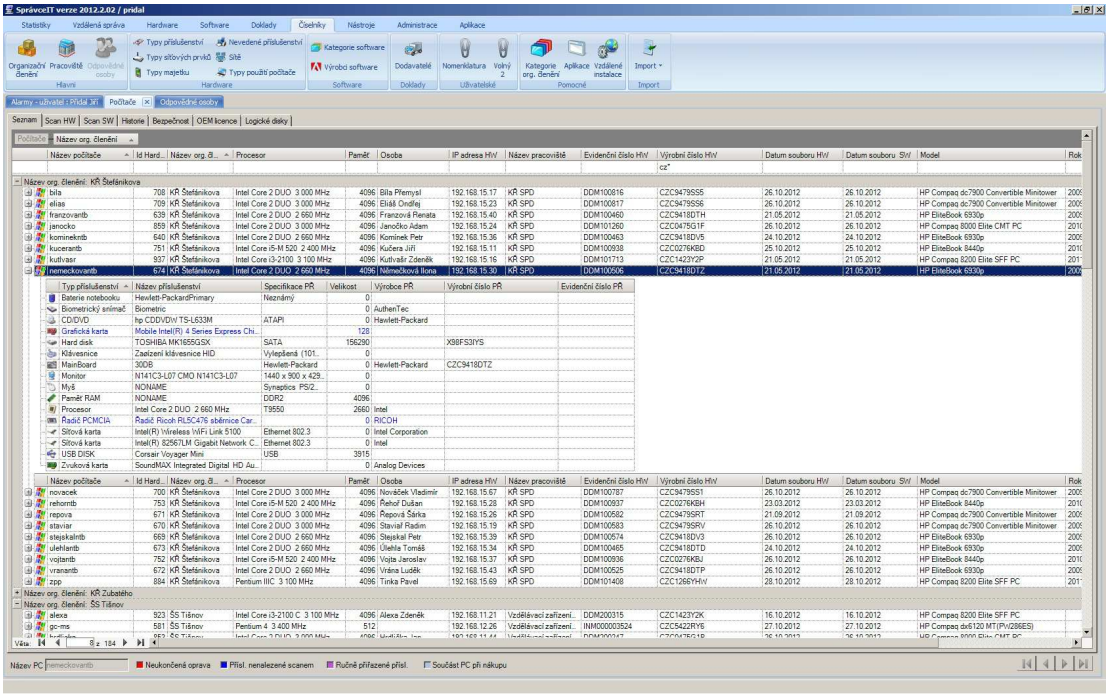
Obrázek 12: Okno v programu EMC Avamar
Zdroj: [25]

5.10. Systém Micos Správce IT

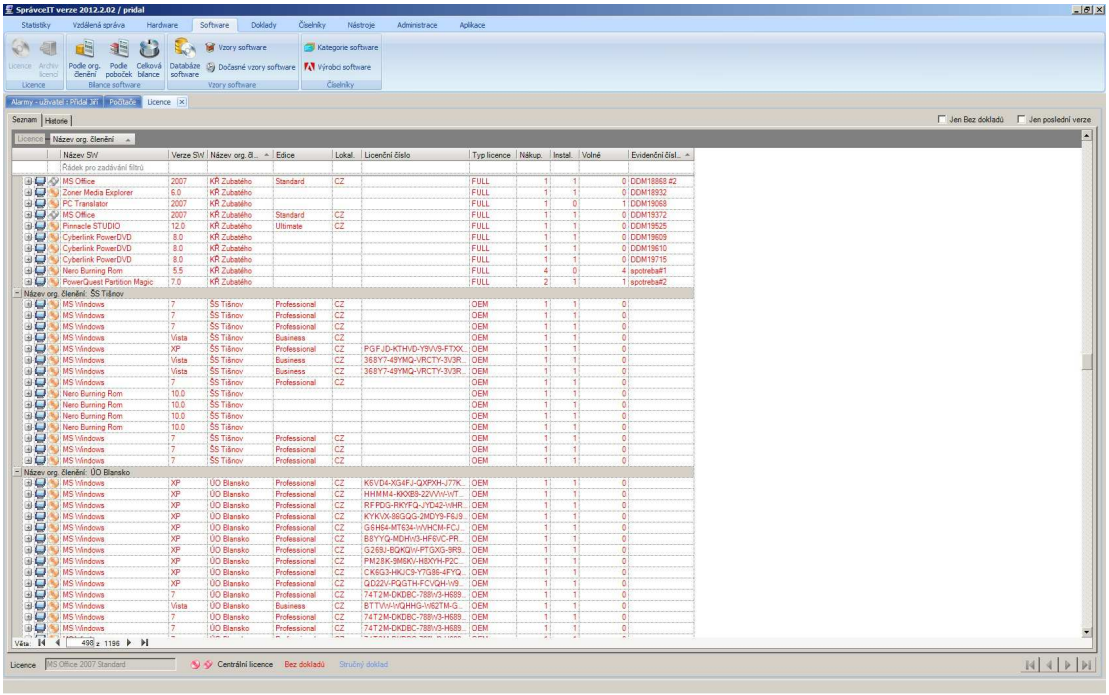
Micos Správce IT je specializovaný systém pro Software Asset Management (SAM). Je určen pro SW audit, správu licencí *(viz. obr. 13)*, HW audit a evidenci výpočetní techniky *(viz. obr.12)*. Systém Správce IT je vyvíjen od r. 1992 a řadí se tak ke špičce programů, které lze využít pro inventuru počítačů a instalovaného software.

- **Výhody systému:**

- Rychlá a snadná instalace;
- Okamžitý přehled o stavu SW a HW vybavení;
- Jednoduché a přívětivé uživatelské rozhraní;
- Automatizace procesů kontroly bez nutnosti obcházení počítačů a obtěžování uživatelů;
- Vlastní systém kontroly bez zásahu externích firem;
- Možnost propojení s aplikacemi Aktivity a HelpDesk;
- Správce IT je atestovaným řešením na shodu s požadavky usnesení vlády č.624/01. [18]



Obrázek 13: Okno Správce IT – PC stanice
Zdroj: [25]



Obrázek 14: Okno Správce IT – Licence
Zdroj: [25]

5.11. Pult centrální ochrany (PCO)

Pult centrální ochrany neboli PCO je služba nabízená soukromými společnostmi. Tato společnost má vybudované své dispečerské stanoviště, které neustále střeží objekty zabezpečené pomocí elektronické zabezpečovací signalizace (EZS), nebo elektronické požární signalizace (EPS) které jsou na pult připojeny. Při vyhlášení poplachu PCO se ihned kontaktuje PČR nebo HZS k výjezdu na místo události (záleží na typu události).

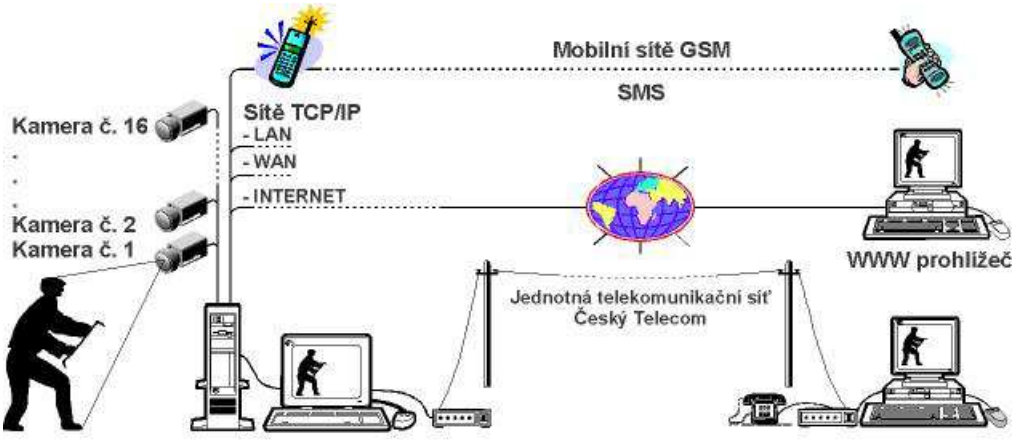
PCO funguje na principu třístranné dohody. Firma, která danou bezpečnostní službu chce využívat platí za poskytnuté služby. Firma, která zabezpečuje PCO pro firmu , která o službu zažádá, si strhává z placené částky provizi za zprostředkování a dohled.

Zbytek částky jde vykonavateli služby v rámci PCO – zde konkrétně HZS JMK.

Pro HZS JMK je částka vedena jako příjem, jež jeden z mála není odváděn do státního rozpočtu.

Pro HZS JMK službu PCO zajišťuje firma Patrol z Jihlavy. Firma Patrol aktuálně provozuje krajské pulty centralizované ochrany u hasičských záchranných sborů HZS kraje Vysočina, HZS Jihomoravského kraje a HZS Středočeského kraje. [20]

Obrázek 15: PCO firmy Patrol
Zdroj: [20]



Obrázek 16: Kamerový systém PCO
Zdroj: [23]

Obrázek 17: Schéma PCO
Zdroj: [15]

5.12. SWOT analýza IS

SWOT analýza je univerzální analytická technika zaměřená na zhodnocení vnitřních a vnějších faktorů ovlivňujících úspěšnost organizace nebo nějakého konkrétního záměru (například nového produktu či služby).

SWOT je zkratka z počátečních písmen anglických názvů jednotlivých faktorů:

- **Strengths** - silné stránky;
- **Weaknesses** - slabé stránky;
- **Opportunities** – příležitosti;
- **Threats** – hrozby. [21]

Vzájemným propojením faktorů silných a slabých stránek na jedné straně vůči příležitostem a hrozbám na druhé straně lze získat nové informace, které charakterizují a hodnotí úroveň jejich vzájemného střetu. [22]

Obrázek 18: SWOT Analýza
Zdroj: [22]

- ***A - Silné stránky***

A1 – fungování celoplošně TCTV 112;

A2 – fungování přenosu datové věty z TCTV 112;

A3 – existuje mnoho zkušeností s rozsáhlým IS;

A4 – existence standardů (registry ÚIR, RES…);

A5 – existence státní mapovací; agentury (ČÚZK) a státních mapových děl.

- ***B - Slabé stránky***

B1 – IS systémy složek jsou na různém stupni vývoje;

B2 – IS jsou nekompatibilní;

B3 – existují duplicitní datové struktury i funkcionality v rámci jednotlivých IS a tím dochází ke zvyšování nákladů;

B4 – standardizace je procesně i organizačně složitý proces.

- ***C - Příležitosti***

C1 – optimalizovat a standardizovat datové zdroje;

C2 – provést optimalizaci procesů;

C3 – optimalizovat investiční náklady;

C4 – optimalizovat provozní náklady;

C5 – redukovat nároky na organizaci.

- ***D - Hrozby***

D1 – podpora divergentních řešení znemožní jakoukoliv optimalizaci;

D2 – neúspěchem při standardizaci podpora divergence řešení;

D3 – velký růst provozních nákladů;

D4 – znehodnocení investic do IS;

D5 – nedůslednou realizací projektů se IZS stane „rukojmím“ dodavatelů.

6. Analýza problému

Bezpečnostní rizika IS

Analýzu bezpečnostních rizik informačního systému HZS JMK jsem provedla na základě dostupných poznatků, informací a materiálů dodaných zástupci HZS JMK. Výstup zpracované analýzy tvoří analýzu rizik IS. Analýza rizik IS popisuje současnou bezpečnostní situaci při zpracovávání dat v provozovaných informačních systémech HZS JMK.

Výsledky rozboru zaměřené na bezpečnost byly zpracovány pomocí konzultací se zaměstnanci a vlastního pozorování a možnosti nahlédnutí do různých aplikací v systému a vnitropodnikových materiálů (*viz. zdroje 25, 26, 27*).

6.1. Hodnocení a zvládání rizik

Analýza rizik věnovaná bezpečnosti informačního systému HZS JMK dosud nebyla provedena. Za řízení rizik v rámci odboru nebo oddělení je zodpovědný jeho vedoucí pracovník.

6.2. Bezpečnostní politika a podpora vedení

Vlastní bezpečnostní politika ICT na HZS JMK není dokumentována. Část požadavků na bezpečnost ICT je uvedena v rámci dokumentu HZS JMK. Tato směrnice však dostatečně nepokrývá všechny aspekty bezpečnosti ICT.

6.2.1. Řízení bezpečnosti ICT

Na HZS JMK bezpečnost IS zabezpečuje IT oddělení na KŘ a na KOPIS. Není zřízena konkrétní funkce správce či manažera bezpečnosti ICT, který by zajišťoval činnosti související s informační bezpečností.

6.2.2. Identifikované zranitelnosti

- ***Neexistující bezpečnostní politika***

Neexistující bezpečnostní politika otevírá nebezpečnou trhlinu v ochraně dat organizace. Není-li přesně stanoveno, co a před čím chránit, nelze ani stanovit způsob odpovídající ochrany IS, pravidla kontroly jejího dodržování a vyvození důsledků, včetně nápravných a preventivních opatření. To vše by měla na základě zjištění analýzy rizik obsahovat právě bezpečnostní politika.

6.2.3. Nedokumentovaná potřebná bezpečnostní pravidla

Neexistence potřebné bezpečnostní dokumentace, předpisů, dokumentovaných procesů a postupů, jež by zabezpečily jednoznačnost výkladu v současné době zatím ještě nevypracované bezpečnostní politiky, pevně stanovená pravidla a systematické řešení bezpečnostních otázek ICT v HZS JMK představují zranitelnost zejména vůči lidskému faktoru.

6.3. Organizační a administrativní bezpečnost

6.3.1. Dostupnost dokumentace, prokazatelnost seznamování

Veškerá existující dokumentace (interní směrnice a nařízení HZS JMK) je dostupná pracovníkům HZS JMK prostřednictvím intranetu.

Za seznámení zaměstnanců s relevantními, nově vydanými (aktualizovanými) předpisy zodpovídají vedoucí příslušných odborů, kteří rovněž provádí kontrolu jejich dodržování.

Seznámení s obsahem daného interního předpisu k příslušnému datu potvrzují zaměstnanci svým podpisem.

6.3.2. Bezpečnost ve vztazích se třetími stranami

Nejsou dokumentována ucelená pravidla pro zabezpečení výpočetní techniky před únikem dat nepovolaným osobám v průběhu implementace, správy, údržby a oprav VT, outsourcingu ap.

Aspekty spolupráce se třetími stranami jsou ošetřeny smluvně, zabezpečení pak vyplývá přímo ze smlouvy, případně z jejího dodatku.

6.3.3. Identifikované zranitelnosti

- ***Neřešena struktura řízení bezpečnosti ICT***

Zabezpečení IS HZS JMK vyžaduje, aby byla bezpečnost IS/ICT systematicky řízena pomocí předem stanovených pravidel a stanovením bezpečnostní struktury a hierarchie řízení, povinností a zodpovědností jednotlivých subjektů. Vytvoření struktury řízení bezpečnosti IS/ICT by mělo být začleněno jako součást budování informačního managementu, případně managementu ICT.

- ***Nestanovena zodpovědná funkce bezpečnostního manažera / správce ICT***

K řízení bezpečnosti ICT je zapotřebí ustanovit především řídícího manažera, jenž zajišťuje nezbytnou funkci bezpečnostního správce zodpovědného za řízení bezpečnosti, který zpracovává a aktualizuje bezpečnostní dokumentaci, aktivně dohlíží na dodržování bezpečnostní politiky/směrnic, kontroluje shodu se skutečností a poskytuje potřebné informace vedení HZS JMK.

6.3.4. Aktiva

Pro potřebu zabezpečení informací je třeba definovat všechna aktiva informačního systému HZS JMK. Za aktiva jsou považovány všechny hmotné i nehmotné součásti informačního systému, včetně HW, SW a lidských zdrojů, které vytvářejí hodnoty zpracovávané a ukládané v IS.

Mezi aktiva, jichž se týká analýza rizik IS, patří například:

fyzická aktiva – veškeré HW vybavení, počítače, sítě, technická zařízení, budovy a ostatní vybavení, dodávky energie, vody, tepla, klimatizace, osvětlení;

softwarová aktiva – programové vybavení, operační systémy, technologie, SW aplikace a dílčí (samostatné) informační systémy, agendy, zdrojové kódy aplikací vyvíjených externími dodavateli, speciální systémy a jejich nastavení;

informační aktiva – veškerá data, informace a údaje zpracovávané v IS HZS JMK;

lidské zdroje (vědomosti, kvalifikace, vynaložená školení, vzdělávání), know-how, dobré jméno HZS JMK;

služby – služby pro veřejnost, resp. pro zaměstnance HZS JMK.

Aktiva IS HZS JMK byla identifikována a ohodnocena na základě informací získaných v průběhu analýzy a konzultací s pověřenými zástupci HZS JMK.

Na základě provedené analýzy byla identifikována a ohodnocena následující aktiva HZS JMK. Přehled těchto aktiv spolu s určením jejich vlastníků je uveden v následující tabulce:

Tabulka 1: Aktiva HZS JMK
Zdroj: [27]

Skupina	č.	Název	Vlastník aktiva
Fyzická aktiva	1.	HW stanice (PC, tiskárny, skenery)	Administrátor
	2.	HW servery (včetně zálohovacích zařízení, diskové pole)	Administrátor
	3.	Přenosná zařízení (notebooky, PDA, média) vně chráněného prostředí	Administrátor
	4.	Ostatní prostředky a zařízení výp. techniky (kabeláž, komunik. zařízení, síťové prvky, UPS)	Administrátor
SW aktiva	5.	Licence za SW (smlouva, listina, fyzická licence, identifikační klíče)	Administrátor
	6.	Nastavení systémů (konfigurace)	Administrátor
Informační aktiva (pouze data)	7.	Aplikace a agendy personální a mzdové	Dle jednotlivých aplikací
	8.	Elektronická pošta	Dle charakteru dat zpracovávaných elektronickou
	9.	Pracovní data uložená na serverech (intranet, sdílená úložiště odborů, home adresáře uživatelů)	Dle konkrétních dat (zpravidla autor dat)
Lidské zdroje (znalosti,zastu-pitelnost)	10.	Administrátoři, správci aplikací (zastupitelnost, znalosti)	-
	11.	Důvěryhodnost HZS JMK (dobré jméno)	Ředitel HZS JMK
	12.	Know-how, pracovní postupy, zavedené	Ředitel HZS JMK

6.3.5. Vlastnictví a vlastníci aktiv

S identifikací aktiv HZS JMK souvisí také určení osob/funkcí (nazývaných obecně „vlastníci“), jež nesou zodpovědnost za daná aktiva nebo skupiny aktiv. Tito vlastníci zpravidla plní roli vedoucích zaměstnanců pověřených zodpovědností za svěřená aktiva. Mají potřebné znalosti o charakteru těchto aktiv a schopnosti posoudit jak jejich hodnotu pro HZS JMK, tak požadavky na ochranu, dostupnost, obnovu, zálohování, ukládání, zpracování a prioritu.

6.3.6. Charakter zpracování dat v rámci IS

Informační systém HZS JMK zpracovává zejména data nezbytná k provozu a řízení HZS JMK, jeho ekonomického zázemí, personalistiky, účetnictví a mzdové agendy atd. Tyto údaje pocházející od HZS JMK či uložené v rámci IS HZS JMK mají v mnoha případech charakter chráněných údajů HZS JMK nebo osobních údajů, na které se vztahuje zákon o ochraně osobních údajů č. 101/2000 Sb., v platném znění. [29]

Z tohoto zákona vyplývají nejen práva, ale také povinnosti při zpracování těchto údajů, a to jak v papírové, tak i v elektronické podobě. Tento zákon definuje ochranu informací pouze na obecné úrovni. Konkrétní způsob zabezpečení informací je dán technickými nebo právními prostředky a způsobem správy IS.

6.3.7. Klasifikace dat a přístup k datům

Jednotlivé odbory si každý samostatně vlastním způsobem řídí informační aktiva spadající do oblasti jejich působnosti, ovšem není schválen obecný postup řízení těchto aktiv. Vlastnictví dat zpravidla připadá vedoucímu zaměstnanci příslušného odboru/oddělení.

Data vyskytující se v informačním systému HZS JMK nejsou klasifikována či řazena do klasifikačních skupin/tříd. Rozlišovány jsou pouze osobní údaje dle zákona č. 101/2000 Sb., o ochraně osobních údajů. [29]

6.3.8. Identifikované zranitelnosti aktiv

- ***Nedefinovaná a neohodnocena aktiva a jejich vlastníci***

Identifikace aktiv HZS JMK je potřebná pro určení jejich hodnoty, následně také pro zjištění a výpočet míry rizika ohrožujícího daná aktiva a stanovení priorit jednak pro zabezpečení aktiva, jednak pro potřeby obnovy aktiva po mimořádné události.

HZS JMK dosud neměl definována a ohodnocena aktiva IS a jim přiřazené vlastníky, definice a hodnocení aktiv je předmětem analýzy rizik.

- ***Nedefinovaná rizika a jejich míra***

Rizika ohrožující aktiva IS HZS JMK musí být identifikována z toho důvodu, aby na jejich eliminaci bylo možno přijmout odpovídající protiopatření a současně stanovit priority pro realizaci těchto opatření, která by měla pokrýt přednostně ta nejkritičtější rizika.

- ***Neexistující klasifikace informací pro jednotlivé skupiny informačních aktiv***

Pro zabezpečení informačních aktiv by měla být tato aktiva rozčleněna do několika kategorií a ke každé kategorii následně přiřazena adekvátní ochranná opatření, aby byla zajištěna odpovídající bezpečnost pro každou kategorii informací různého stupně citlivosti.

6.4. Personální bezpečnost

6.4.1. Bezpečnostní požadavky pro uchazeče o zaměstnání

Výběr vhodných kandidátů na pracovní místa probíhá v souladu s interními předpisy, zejména pak Pracovním řádem, formou výběrového řízení.

6.4.2. Povinnosti zaměstnanců

Povinnosti zaměstnanců jsou uvedeny v Pracovním řádu a v příslušné legislativě. Některé konkrétní povinnosti jsou rozpracovány ve směrnicích a interních nařízeních a předpisech HZS JMK, ty se však nevěnují informační bezpečnosti IS/ICT komplexně.

6.4.3. Vzdělávání a školení

Postupy a aktivity spojené se vzděláváním a školením v oblasti ICT a bezpečnosti ICT nejsou zdokumentovány.

Dále jsou zaměstnanci povinni absolvovat každoroční školení BOZP a požární ochrany.

6.4.4. Nástup/odchod zaměstnance

Přístupová práva do IS (vytvoření účtu, definice přístupových práv), přidělení konkrétního HW/SW a pracoviště je úzce provázána na danou pracovní pozici. Pevně stanovené postupy pro nástup/odchod zaměstnance, nejsou k dispozici.

6.4.5. Identifikované zranitelnosti

- ***Nedostatečné školení uživatelů v oblasti informační bezpečnosti***

Zejména opomíjené průběžné školení zohledňující neustálý vývoj v oblasti bezpečnosti ICT spolu s neustálou potřebou vzdělávat se v této oblasti představuje zranitelné místo HZS JMK potažmo IS.

6.5. Fyzická (objektová) bezpečnost a bezpečnost prostředí

U hlavního vstupu do budovy je zřízena recepce, kde je povinností návštěvníka se zapsat do evidence (jméno a příjmení, doba příchodu a odchodu, jméno navštíveného, příp. název organizace.

Přístup do většiny kanceláří je řízen zejména pomocí klíčového režimu. Při odchodu posledního pracovníka z kanceláře by měl tento uzamknout danou místnost. Je však pravidlem, že jsou zamykány pouze dveře do chodby a průchody mezi kancelářemi se nechávají otevřené.

6.6. Řízení komunikací a provozu

6.6.1. Provozní postupy a odpovědnosti

Provozní postupy pro provoz IS jsou zdokumentovány jen částečně.

6.6.2. Ochrana proti škodlivým kódům

Ochrana IS před škodlivými kódy je zajištěna prostřednictvím antivirového programu, a to na uživatelských stanicích i na serverech. Uživatelé nemohou měnit nastavení antiviru na svých stanicích a antivirus je plně centrálně řízen.

Skenování pracovních stanic probíhá v reálném čase a podléhají mu všechny soubory podle aktuální virové masky.

6.6.3. Zálohování

Zálohování dat u HZS JMK je prováděno pomocí systému Avamar. Data jsou ukládána na příslušné servery. Veškerá důležitá data by měla být tedy v těchto úložištích, která podléhají centrálnímu zálohování. (*Viz. kapitola 5.9.)*

Zálohování probíhá denně**,** vždy v noci (7 x týdně).

Lokální stanice se centrálně nezálohují, záleží na uvážení uživatelů, zda si svá data zálohují.

Instalační CD/DVD jsou zálohována formou ISO image uložených na určeném serveru. Originální instalační média CD/DVD jsou uložena u administrátora.

6.6.4. Správa sítě HZS JMK

Správa části serverů je prováděna dodavatelskou firmou – výjezdový systém (Spojař - *viz. kapitola 5.6.*). Podmínky správy, povinnosti a odpovědnosti dodavatele jsou předmětem smlouvy.

HZS JMK nemá instalovány IDS/IPS systémy.

6.6.5. Dokumentace konfiguračních nastavení systémů

Část konfiguračních nastavení IS HZS JMK je vedena administrátorem.

Dále není řízen přístup k této dokumentaci a není ani způsob jejího uchovávání a ochrany.

6.6.6. Bezpečnost přenosných zařízení

V IS HZS JMK jsou ve velké míře využívány notebooky. Na ochranu těchto zařízení a dat na nich uložených nejsou přijata žádná další bezpečnostní opatření. Na přenosných zařízeních není používán SW pro šifrování dat.

6.6.7. Bezpečnost při zacházení s médii

Na HZS JMK jsou hojně využívána výměnná média (CD/DVD, ojediněle i diskety) a USB flash disky. Bezpečnostní pravidla pro zacházení s těmito médii a daty na nich uloženými stanovena nejsou.

6.6.8. Bezpečná likvidace dat

Skartace dat se provádí dvojím způsobem :

- Při vyřazení počítače nebo změny uživatele se provede zformátování disku Uživatelé SW pro bezpečnou skartaci dat nepoužívají;
- Fyzická skartace CD / DVD s citlivými daty, poté co již data nejsou aktuální nebo potřebná (vypršené licence programů, atd.).

6.6.9. Monitorování a logování

Aktivity správců systémů jsou zaznamenávány formou logů, díky kterým lze zpětně dohledat aktivitu konkrétního uživatele v systému.

6.6.10. Identifikované zranitelnosti

- ***Nedostatečně řízena dokumentace kritických konfiguračních nastavení systémů***

Částečně jsou zdokumentovány konfigurace a nastavení jednotlivých kritických systémů (serverů, síťových prvků ap.). Některá dokumentovaná nastavení nejsou aktuální.

Dále nejsou stanoveny podmínky uchovávání a definována pravidla přístupu (oprávnění) k této dokumentaci.

- ***Neprovádění testů obnovy ze záloh***

V rámci systému zálohování nejsou prováděny pravidelné testy funkčnosti záloh, což může vést v případě nutnosti obnovení k nefunkčnosti části IS, v případě havárie většího rozsahu dokonce i celého IS.

6.7. Řízení přístupu

Politika řízení přístupu není implementována. Postup pro zřízení/zrušení uživatelského účtu a přidělování/změnu/odebrání přístupových práv uživatele není definován.

6.7.1. Řízení přístupu uživatelů

Uživatelé přistupují k IS HZS JMK prostřednictvím svého přiděleného účtu. Účty vytváří a oprávnění nastavuje administrátor. Z důvodu bezpečnosti jsou uživatelům přidělována jen nezbytně nutná oprávnění.

6.7.2. Řízení privilegovaného přístupu

Administrátorské účty podléhají běžným pravidlům pro heslo (nejsou nastavena přísnější pravidla). Administrátorský účet je používán pouze pro administrátorské účely.

6.7.3. Politika hesel

Heslo pro první přihlášení uživatelů není uživatel nucen po prvním přihlášení heslo změnit.

6.7.4. Řízení přístupu k síti a k internetu

Uživatelé využívají standardní služby internetu jako jsou www, služby elektronické pošty (e-mail). Některé služby jsou z bezpečnostních důvodů zakázány. Není definován postup pro povolování (schvalování) služeb internetu.

6.7.5. Řízení externího připojení

Vzdálený přístup k IS HZS JMK je umožňován k elektronické poště prostřednictvím šifrované komunikace – HTTPS, na základě zadání uživatelského jména a hesla.

Vzdálený přístup je využíván i pro správu serverů, autentizace probíhá rovněž na základě ověření uživatelského jména a hesla.

Pro vzdálenou komunikaci mezi HZS JMK a ostatními organizacemi (bankovní instituce, ČSSZ) jsou používány digitální certifikáty dle požadavků organizace (kvalifikované certifikáty, resp. certifikáty vydané certifikační autoritou dané organizace).

6.8. Nákup, vývoj a údržba IS

Systém plánování by měl zahrnovat dokumenty typu plán rozvoje, plán činnosti ap., které jsou závislé na stanoveném rozpočtu a ovlivňují jeho tvorbu na následná období v závislosti na definovaných potřebách.

Jako podklad pro plánování rozvoje IS a efektivního využívání prostředků výpočetní techniky, komunikačních technologií a SW aplikací slouží obvykle průběžné vyhodnocování monitoringu provozu a zatížení sítě, požadavků jednotlivých odborů a také strategických plánů v oblasti IT.

6.8.1. Kryptografická opatření

HZS JMK nemá uceleně řešen systém PKI. Vybraní zaměstnanci mají certifikáty kvalifikovaných certifikačních autorit, a to zejména pro komunikaci s externími organizacemi (ministerstva, bankovní instituce, Česká správa sociálního zabezpečení apod.).

6.8.2. Bezpečnost systémových souborů

Na lokální stanice je instalován standardní image obsahující celoplošně používané aplikace/systémy (OS, kancelářský balík MS Office apod.). Na základě žádosti jsou pak konkrétní aplikace související s pracovní náplní uživatele administrátorem doinstalovány.

6.8.3. Bezpečnost v procesu vývoje

Vývoj aplikací, SW, případně dalších částí informačního sytému na zakázku není v prostředí HZS JMK příliš rozšířen. Většinou jsou využívány konkrétní komerční produkty.

6.8.4. Podpora uživatelů

Podpora uživatelů je řešena formou telefonické nebo emailové podpory, případně osobního zásahu administrátorem na PC uživatele.

6.9. Řízení bezpečnostních incidentů

6.9.1. Hlášení bezpečnostních incidentů

Na HZS JMK není oficiálně definováno, co je považováno za bezpečnostní incident. Uživatelé v současné době nemají povinnost hlásit bezpečnostní incidenty a nejsou v této oblasti ani proškoleni.

Bezpečnostní incidenty tak bývají hlášeny jen výjimečně a nejsou ani systematicky vyhodnocovány.

6.9.2. Identifikované zranitelnosti

- *Absence pravidelného vyhodnocování bezpečnostních incidentů*

Hlášení závad a poruch prostřednictvím stávajících prostředků je způsob, jakým nelze evidovat, řešit a také vyhodnocovat mimořádné události, mj. také bezpečnostní incidenty, jelikož uživatelé nemusí být schopni rozpoznat běžnou závadu od bezpečnostního incidentu.

HZS JMK nemá funkční systém evidence, řešení a vyhodnocování těchto incidentů.

6.10. Řízení kontinuity

Cílem řízení kontinuity činností HZS JMK je ochrana kritických činností a procesů před přerušením následky závažných chyb a katastrof.

V IS HZS JMK nejsou v současné době identifikovány procesy kritické pro činnost HZS JMK. Není zaznamenáno do jaké míry jsou procesy IT závislé na podpoře informačního systému.

6.10.1. Identifikované zranitelnosti

- ***Nedostatečné řízení kontinuity systémů***

Nejsou definována ani hodnocena rizika pro jednotlivá aktiva. Dosud nebyla provedena analýza dopadů - Business Impact Analysis (BIA). Nejsou kategorizovány činnosti z hlediska kontinuity procesů v ICT, jejich kritičnosti, priorit obnovy apod.

- ***Neexistence havarijních plánů***

Neexistují havarijní plány a plány zachování kontinuity pro případ havárie a nehody - výpadek proudu, požár, únik vody a jiné fyzické příčiny (selhání hardwaru i softwaru).

6.11. Soulad s požadavky

6.11.1. Audit informační bezpečnosti

Samostatný audit zaměřený na bezpečnost IT dosud proveden nebyl. Shoda skutečnosti s postupy stanovenými interními směrnicemi a předpisy je nepravidelně kontrolována vedoucími pracovníky.

6.11.2. Legislativa

Sledováním změn legislativy ani kontrolou shody obecně platných legislativních předpisů se skutečností není nikdo pověřen. Částečně se tímto zabývají právníci HZS JMK v rámci výkonu své pracovní činnosti a to především:

- Usnesení vlády České Republiky č. 624/2001 Sb., o pravidlech, zásadách a způsobu zabezpečování kontroly užívání počítačových programů; [24]
- Zákon č. 365/2000 Sb., o informačních systémech veřejné správy; [32]
- Zákon č. 101/2000 Sb., o ochraně osobních údajů. [29]

6.11.3. Identifikované zranitelnosti

- ***Absence provádění auditu bezpečnosti IT/ICT***

Nebyl proveden vnitřní ani vnější audit zaměřený na bezpečnost IT. Audity zaměřené na IT se také neprovádějí.

6.12. Zranitelná místa v IS

Zranitelná místa v IS HZS JMK představují všechny slabiny systému, jež jsou potenciálně zneužitelné uvedenými hrozbami a umožňují průnik, poškození, ztrátu nebo zneužití IS k neoprávněným zásahům a jiné škodlivé činnosti.

Zranitelná místa, jež ohrožují většinu informačních systémů a nevyhýbají se ani analyzovanému systému HZS JMK, jsou uvedena v následující tabulce:

Tabulka 2: Zranitelná místa IS HZS JMK
Zdroj: [27]

Oblast bezpečnosti (dle ISO/IEC 27002)	Název zranitelnosti
Bezpečnostní politika	Neexistující bezpečnostní politika
Bezpečnostní politika	Nedokumentována potřebná bezpečnostní pravidla používání ICT (povinnosti a odpovědnosti uživatelů/zaměstnanců)
Organizační bezpečnost	Nestanovena zodpovědná funkce/role bezpečnostního manažera/správce za ICT
Klasifikace a řízení aktiv	Nedefinována rizika a jejich míra
Klasifikace a řízení aktiv	Nedefinována a neohodnocena aktiva a jejich vlastníci
Klasifikace a řízení aktiv	Neexistující klasifikace informací pro jednotlivé skupiny informačních aktiv
Personální bezpečnost	Nedostatečné školení uživatelů v oblasti informační bezpečnosti
Řízení komunikací a provozu	Nedostatečně řízena dokumentace kritických konfiguračních nastavení systémů
Řízení přístupu	Nedostatečná politika hesel a správy účtů
Řízení kontinuity činností	Neexistence havarijních plánů IS/ICT
Řízení kontinuity činností	Nedostatečné řízení kontinuity systémů
Zvládání bezpečnostních incidentů	Absence pravidelného vyhodnocování bezpečnostních incidentů

7. Vlastní návrhy řešení

Mezi hlavní prvky ke zlepšení současné situace jsou návrhy, které by pomohly zlepšit celkovou situaci z hlediska zabezpečení a propojenosti IS. Ulehčení a zefektivnění práce v IS jak pro uživatele tak i pro lepší, rychlejší a ucelenější informace a přístup k potřebným datům.

Navrhnuto na základě vlastního průzkumu, vnitropodnikových materiálů, konzultací na KŘ HZS JMK, vypracované analýzy rizik IS a zpracované SWOT analýzy.

7.1. Zavedení bezpečnostní politiky

Návrh na změnu vyplývá na základě analýzy rizik a zjištění, že neexistující bezpečnostní politika může způsobit velmi vážná ohrožení v ochraně dat.

Zavedení bezpečnostních pravidel a uvedení je do užívání, může v mnoha případech zabránit zneužití dat neoprávněným osobám.

Je třeba přesně stanovit stupně důležitosti a utajení dat a určit k danému stupni potřebnou úroveň zabezpečení *(viz. 5.12. – SWOT B1, B2, D1, D2).*

- **VÝHODY**

1) IS by byl celkově zabezpečenější proti zneužití a neoprávněným vstupům do systému.

2) Díky přísnějším a propracovanějším určením přístupu k datům, by se v systému dalo snadno zpětně dohledat a sledovat přístupy do systému díky osobnímu přístupovému heslu, které by bylo pro každého uživatele unikátní.

- **NEVÝHODY**

1) Velmi náročná implementace, jelikož změny v opatření by se musely projevit v celém IS a tudíž i pro každou databázi a aplikaci by byla nutnost tvořit nová pravidla a přístupová hesla.

2) V současné situaci je návrh bohužel prakticky nerealizovatelný, protože by to vyžadovalo kompletní obměnu celé struktury IS HZS JMK. Jelikož systém pro HZS JMK je natolik specifický, tak v současné době realizace návrhu není možná.

3) Kvůli velmi náročné implementaci by byly změny jak časově náročné, tak i finančně náročné. Jelikož HZS je z převážné části financován Ministerstvem vnitra ČR, návrh by zasáhl do státního rozpočtu.

7.2. Provázání IS

V současné době jsou v rámci HZS JMK dva samostatně fungující systémy – ekonomický a výjezdový. Výjezdový systém je velmi rozsáhlý a obsahuje několik dílčích databází, které běží pod databázovým systémem Oracle. Příkladem je program *Spojař (viz. kapitola 5.6.)*

Celkové provázání IS se všemi databázemi a aplikacemi by umožnilo efektivnější práci s daty, rychlejší zpracování informací a také kontrolovatelný přístup do systému, čímž by se daly dohledat zpětně přístupy uživatelů do systému a tím i eliminovat neoprávněné vstupy do systému.

Díky propojenosti IS by data k následnému zpracování i správě byla ucelenější a přehlednější *(viz. kapitola 5.12. – SWOT B3, B4, C1, C2, C4, D3).*

Při realizaci návrhu by rozsáhlejší stávající systém byl zachován a postupně by se data z druhého sytému převáděla, tak aby v konečné fázi vznikl pouze jeden komplexní a ucelený systém *(viz. kapitola 4.1.)*.

- **VÝHODY**

1) Díky propojenosti systémů by se snížily náklady na správu systému.

2) Celková propojenost by usnadnila práce s daty v aplikacích i v databázích a zefektivnění práce uživatelů i správců sítě, díky ucelenosti dat,

3) Kontrolovatelný přístup do systému a eliminace neoprávněných vstupů.

- **NEVÝHODY**

Jelikož v současné době má HZS JMK dva samostatné systémy a to ekonomický a výjezdový, byla by integrace dat časově velmi náročná.

7.3. Pravidelné proškolování uživatelů IS

Je potřebné, aby každý uživatel IS, který jakýmkoliv způsobem zasahuje do systému nebo pracuje s daty, byl pravidelně proškolován o bezpečnosti IS a také uživatele seznámit jak se systémem správně pracovat a docílit tak efektivnější práce s daty *(viz. kapitola 5.12. – SWOT C5).*

Pravidelné školení uživatelů je potřebné i z důvodu občasných změn struktury nebo formy databází v systému.

Důležitým důvodem, proč uživatele seznamovat s novými poznatky, postupy a bezpečnostními pravidly je zajistit bezpečnější přístup do systému z hlediska možnosti případného zneužití dat nebo neoprávněného vstupu do systému nepovolaným osobám. Uživatelům dát návod :

- Jak těmto hrozbám zamezit;
- Jak používat správně hesla pro přístup do systému;
- Jak správně zacházet s dostupnými daty a databázemi.

- **VÝHODY**

1) Zamezení neoprávněných vstupů k utajeným datům nepovolaným osobám.

2) Lepší informovanost uživatelů o způsobech neoprávněného přístupu do systému.

3) Svědomitější nakládání s přístupovými hesly do systému.

4) Vyvarování se častých uživatelských chyb o bezpečnosti.

5) Správně motivovaní uživatelé mají zájem o dodržování bezpečnostních pravidel a tudíž i lepší pracovní výkonnost a efektivnější zpracování dat.

6) Kvalitnější vyhodnocování událostí.

- **NEVÝHODY**

1) Proškolování uživatelů je časově náročné, jelikož při současném stavu ve směnovém provozu by se školení muselo provádět na několik etap aby obsáhlo všechny potřebné uživatele.

2) Velkou klíčovou překážkou je neochota uživatelů spolupracovat, učit se nové postupy a měnit zavedené návyky, takže nové informace a požadavky na bezpečnost ignorují.

8. Zhodnocení návrhů

V celkovém zhodnocení výše uvedených návrhů na zlepšení budou posuzovány dvě hlediska. Celková využitelnost a přínosy daných návrhů a ekonomické zhodnocení na realizaci návrhů.

8.1. Využitelnost a přínos návrhů

Při zhodnocení prvního návrhu je využitelnost a přínos do budoucna zlepšení celkové bezpečnosti systému a vypracování ucelených bezpečnostních pravidel jak s IS pracovat. Problémová fáze by nastala při zavádění nových bezpečnostních pravidel a nové stanovení úrovní bezpečnosti a přístupu do systému, jelikož stávající fungující databáze by se musela od základu změnit s veškerými podmínkami při filtraci a asociaci mezi všemi aplikacemi. Nyní to není možné, jelikož nejsou přesně definované úrovně přístupu a tak by změny byly velmi náročné časově i finančně.

Při zhodnocení druhého návrhu na provázání IS je přínos i využitelnost v budoucnu velmi vysoká a v možné budoucí obměně systému by se návrh dle možností realizoval. Změny by umožnily celkové usnadnění, zrychlení zpracování a vyhodnocení informací, což velmi často hraje významnou roli pro záchranné složky.

Při zhodnocení třetího návrhu na proškolování uživatelů je využitelnost i přínos z hlediska bezpečnosti a lepší informovanosti o IS vítaným návrhem. Správci a administrátoři sítě by návrh na danou změnu velmi uvítali, ale opačný přístup by nastal ze strany uživatelů, kteří se neradi učí nové postupy a

bezpečnostní pravidla jak s IS pracovat. Pokud bude návrh v budoucnu realizován, je otázkou, kolik uživatelů bude ochotno změnit svůj přístup a odpor ke změnám.

8.2. Ekonomické zhodnocení návrhů

Z ekonomického hlediska jsou všechny tři návrhy realizovatelné za předpokladu schválení a vyčlenění finančních prostředků z rozpočtu Ministerstva vnitra ČR ze státního rozpočtu (návrh 1) nebo dotací na vzdělávání zaměstnanců.

Nejsložitější na realizaci a také na vyčlenění finančních prostředků shledávám první návrh, jelikož by bylo třeba zavézt již do funkčního IS nová bezpečnostní pravidla a přístupová hesla, která by bylo třeba kompletně propojit se stávajícím systémem a ke každému uživateli. Pro časovou náročnost by celkové zavedení do systému bylo finančně náročné.

V druhém návrhu by realizace byla velmi vítanou změnou v systému. Finanční náročnost změny by nebyla příliš nákladná, ale z časového hlediska obtížně realizovatelná. Provést kompletní integraci dat by vyžadovalo další zaměstnance, kteří by přesun dat prováděli systematicky aby změny nenarušovaly běžný chod systému.

Ve třetím návrhu by záleželo, zda bude projekt schválen a jakým způsobem by probíhalo proškolování uživatelů. Pokud by školení prováděli interní zaměstnanci HZS JMK, tak finanční náročnost by byla minimální.

Ovšem, pokud by se školení pojalo jako projekt na vzdělávání zaměstnanců přes externí firmu, pak by finanční výdaje byly znatelné pro celkový rozpočet HZS JMK. Školící střediska pro takto specifické požadavky na školení systémů pro veřejnou správu jsou časově i finančně velmi náročné, protože velká část používaného SW u HZS JMK bylo vyvinuto speciálně na zakázku pro HZS JMK *(např. Spojař – viz.kapitola 5.6.)*.

Přehled různých opatření spolu s odhadem jejich finanční náročnosti a priority implementace. Detailní odhad finanční náročnosti závisí na konkrétním způsobu implementace jednotlivých opatření.

Hodnocení předpokládaných nákladů na jednotlivá protiopatření vychází z následující stupnice:

- nízké – řádově do desetitisíců korun - většinou jsou to opatření organizačního charakteru;
- střední – náklady do cca 500 000 Kč;
- vysoké – náklady nad 600 000 Kč.

Hodnocení priority implementace opatření:

- nízká  – opatření pro pokrytí nízkých rizik (pokud není riziko vedením HZS JMK prohlášeno za akceptovatelné), implementace opatření v horizontu 1-2 let;
- střední  – opatření pro pokrytí středně závažných rizik, implementace opatření v horizontu do jednoho roku;
- vysoká  – opatření na pokrytí vysokých rizik, doporučený termín implementace v horizontu 3-6 měsíců.

Tabulka 3: Obtížnost a náklady na implementaci změn v IS
Zdroj: Vlastní (na základě konzultací)

č.	Název	Náklady na realizaci	Priorita implementace
1	Definice bezpečnostní politiky IS a její dokumentace – základ bezpečnosti informačního systému	Nízké až střední (500 000,-)	H
2	Vytvoření funkce správce/manažera bezpečnosti ICT	Nízké až střední (50 000,-)	H
3	Bezpečnostní školení	Nízké až střední (150 000,-)	M
4	Klasifikace dat	Nízké až střední (90 000,-)	M
5	Řízení rizik a jejich míry, plán zvládání rizik	Střední (500 000,-)	M
6	Definice vlastníků aktiv	Nízké (25 000,-)	M
7	Plán zachování kontinuity, havarijní plán IS/ICT	Střední (550 000,-)	M
8	Stanovení a schválení bezpečnostních pravidel pro uživatele	Nízké až střední (350 000,-)	H

Celkové jednorázové náklady na realizace všech návrhů na změny by byly: 2 215 000,- Kč.

Financování HZS spadá pod Ministerstvo vnitra České republiky a tudíž i schválení a vyčlenění finančních prostředků záviselo na uvolnění dané částky ze státního rozpočtu.

Provozní náklady na IS HZS JMK:

Tabulka 4: Náklady na IS HZS JMK
Zdroj: Vlastní (na základě konzultací)

Náklady	Cena
Měsíční náklady na správu bezpečnosti	12 x 50 000,-
Měsíční náklady na provoz linek (27 stanic + KOPIS + KŘ)	12 x cca 200 000,-
Náklady na generální údržbu systému, opravy a obnovy HW komponent	cca 1 000 000,-
Celkové provozní náklady na IS HZS JMK	**cca 4 000 000,-**

Celkové roční provozní náklady na provoz IS HZS JMK jsou přibližně 4 000 000,- Kč.

9. Závěr

V této práci jsem se zabývala možnostmi provozování bezpečného informačního systému HZS JMK s cílem provést analýzu informačního systému Hasičského záchranného sboru Jihomoravského kraje a na základě dané analýzy vytvořit model pro bezpečné provozování uvedeného IS na úrovni manažerského řízení.

Na základě stanovených cílů práce analyzovat IS HZS JMK, vytvořit model pro bezpečné provozování uvedeného IS na úrovni manažerského řízení, provedení průzkumu a celkové zhodnocení stávající situace byly nalezeny nedostatky v rámci bezpečností politiky a provázanosti IS, což má podstatný vliv na komplexní bezpečnost sytému a rychlejší a efektivnější využití práce s informacemi v systému.

Díky zpracovaným návrhům na změny, za předpokladu jejich realizace, by se situace mohla do budoucna změnit a celkové podmínky jak z hlediska bezpečnosti systému, tak zrychlení zpracování dat a přenosu informací z celkového hlediska do budoucna zlepšit

Práce byla zaměřena na popis stávající situace a analýzu řešeného problému v rámci zpracování pomocí softwaru TCTV 112 a HZS JMK a vnitropodnikových materiálů, které mi ke zpracování byly poskytnuty.

Dále bylo zvoleno několik návrhů na zlepšení stávající situace dle zvoleného cíle, kterého má být za pomocí návrhů ke zlepšení dosaženo. Nechybí ani zhodnocení každého návrhu pomocí vyjmenovaných výhod i nevýhod spojených se zavedením změn a také celkové zhodnocení návrhů jak z hlediska využitelnosti a přínosů, tak i z ekonomického hlediska, který je při realizaci projektů důležitým faktorem.

Cílem práce bylo také upřesnit některé bezpečnostní složky z hlediska personální podpory, které byly navrhnuty a zhodnoceny ve vlastních návrzích na zlepšení současné situace *(viz. kapitola 7.3.)*.

Věřím, že tato práce bude inspirací a námětem ke změnám díky zpracovaným návrhům ke zlepšení na základě poskytnutých vnitropodnikových materiálů a provedeného vlastního průzkumu a konzultací na KOPIS HSZ JMK a KŘ HZS JMK.

10. Seznam použitých informačních zdrojů

Literární zdroje

1. HINGSTON, P. *Efektivní marketing*. Praha: Euromedia Group - Knižní klub, 2001. 192 s. ISBN 80-242-0893-8.

2. CHEN, S. *Strategic management of e-business*. Chichester [England]; New York: Wiley, 2005. 366 s. ISBN 0-470-87073-7.

3. JANOUCH, V. *Internetový marketing: prosaďte se na webu a sociálních sítích*. Brno: Computer Press, 2010. 304 s. ISBN 978-80-251-2795-7.

4. KAWASAKI, G. *Umění rozjezdu*. Praha: Pragma, 2010. 216 s. ISBN 978-80-7349-244-1.

5. KOCH, M., DOVRTĚL, J., HRŮZA, T., NENIČKOVÁ, H. *Management informačních systémů*. 3. přepracované vydání. Brno: Akademické nakladatelství Cerm, 2010.

6. LINHART, P. a ŠILHÁNEK, B. *Ochrana obyvatelstva v Evropě.* Praha: MV GŘ HZS ČR, 2005. 196 s. ISBN 80-86640-55-8.

7. LINHART, P. a ŠILHÁNEK, B. *Civilní nouzové plánování v některých zemích, USA a Kanadě.* Praha: MV GŘ HZS ČR, 2007. 104 s. ISBN 978-80-86640-89-1.
8. LINHART, P. a ŠILHÁNEK, B. *Nevládní organizace působící v ochraně obyvatelstva v některých evropských zemích*. 1.vyd. Praha : MV GŘ HZS ČR, 2009. 106 s. ISBN 978-80-86640-87-7.

9. MOLNÁR, Z. *Moderní metody řízení informačních systém*ů. Praha: Grada, 1992, s. 286. ISBN 80-85623-07-2

10. OŠŤÁDALOVÁ, T. *Zavedení tísňové linky 112 v České republice.* 1.vyd. Ostrava: MV GŘ HZS ČR, 2005. 76 s. ISBN: 80-86634-69-8.

11. RYBIČKA, Jiří a kol. *Informatika pro ekonomy*. 4. vyd. KONVOJ Brno, 2008, 147 s. ISBN 978-80-7302-150-4.

12. ŘEPA, Václav. *Analýza a návrh informačních systémů.* 1.vyd. Praha: EKOPRESS, 2000. 185 s. ISBN 80-86119-13-0.

13. SEČKAŘOVÁ, H. *Návrh modelu informačního a komunikačního systému HZS. JMK*. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2010. 53 s.

Ostatní zdroje

14. *EMC Avamar* [online]. [cit. 2013-01-02]. Dostupné z: http://www.emc.com/backup-and-recovery/avamar/avamar.htm

15. *Genova-PCO* [online]. [cit. 2012-12-30]. Dostupné z: http://www.genova.cz/pco-pult-centralni-pozarni-ochrany/

16. *HP Network Node Manager* [online]. [cit. 2013-01-02]. Dostupné z: http://www8.hp.com/us/en/software-solutions/software.html?compURI=1170657#.UJJ3NpZKy-0

17. *Management bezpečnosti* [online]. [cit. 2012-12-30]. Dostupné z: http://managbezp.webnode.cz/kontakt/informacni-system/

18. *Micos Software* [online]. [cit. 2013-01-02]. Dostupné z: http://www.micos-sw.cz/cz/produkty/spravce-it-audit-sw-a-hw-evidence-a-sprava-licenci.html

19. *Mvcr* [online]. 2009 [cit. 2012-12-30.]. Tísňová volání v České republice-Hasičský záchranný sbor České republiky. Dostupné z WWW: http://www.hzscr.cz/clanek/tisnova-volani-v-ceske-republice.aspx

20. *Patrol-PCO* [online]. [cit. 2012-12-30]. Dostupné z: http://www.patrol.cz/pco-pulty-centralni-ochrany.html

21. *SWOT analýza* [online]. [cit. 2012-12-30]. Dostupné z: https://managementmania.com/cs/swot-analyza

22. *SWOT Analýza* [online]. [cit. 2013-01-16]. Dostupné z: http://www.sunmarketing.cz/nastroje/slovnik/swot-analyza

23. *Torex-PCO* [online]. [cit. 2012-12-30]. Dostupné z: http://www.torex-security.cz/strezeni-objektu-pres-kamerovy-pult-centralni-ochrany

24. Usnesení vlády České Republiky č. 624/2001 Sb., o pravidlech, zásadách a způsobu zabezpečování kontroly užívání počítačových programů.

25. Vnitropodnikové materiály. *Software HZS JMK.*

26. Vnitropodnikové materiály. *Software TCTV 112.*

27. Vnitropodnikové dokumenty HZS.*Učební pomůcky, Příručky, Směrnice,Pokyny.*

28. Vyhláška č. 328/2001 Sb., o podrobnostech zabezpečení integrovaného záchranného systému, zaměření rozvoje operačních a informačních středisek integrovaného záchranného systému na úrovni krajů (schváleno poradou vedení MV 2003)

29. Zákon č. 101/2000 Sb., o ochraně osobních údajů

30. Zákon č. 110/1998 Sb., o bezpečnosti ČR

31. Zákon č. 239/2000 Sb., o integrovaném záchranném systému

32. Zákon č. 365/2000 Sb., o informačních systémech veřejné správy;

11. Seznam zkratek a pojmů

112 – Telefonní číslo tísňové linky

Avamar – Zálohovací systém

BOZP – Bezpečnost a ochrana zdraví při práci

EPS – Elektronické požární signalizace

EZS – Elektronické zabezpečovací signalizace

HZS – Hasičský záchranný sbor

ICT – Informační a komunikační technologie

IKIS I. – Aplikace na principu webového rozhraní odkazující se na databázový systém Oracle

IKIS II. – Souhrn aplikačních programů odkazující se na databázový systém Oracle

IS – Informační systém

ISV – Integrovaný systém výjezdů

IZS – Integrovaný záchranný systém

JMK – Jihomoravský kraj

JPO – Jednotky požární ochrany

KOPIS – Krajské operační a informační středisko

KŘ – Krajské ředitelství

Micos Správce IT – Program pro správu HW a SW

Matra – Radiostanice provozující Ministerstvo vnitra České republiky pro potřeby bezpečnostních složek státu.

Network Node Manager – Program pro správu a management sítí

OPIS – Operační a informační středisko

Oracle – Databázový systém pro zpracování dat

PCO – Pult centrální ochrany

PKI – (Public Key Infrastructure) Infrastruktura veřejného klíče

PKV – Příkaz k výjezdu

PO – Požární ochrana

SSU – Statistické sledování událostí

TCTV – Telefonní centrum tísňového volání 112

TTS – Text to speech (software převádějící textovou zprávu do hlasového oznámení, které při vyhlášení poplachu slyší výjezdové jednotky při přípravě k výjezdu)

ZOZ – Zpráva o zásahu

12. Seznam obrázků a tabulek

Obrázky:

Tabulky:

13. Přílohy

Příloha 1: Model realizace projektu

Příloha 2: Základní statistické údaje o činnosti JPO

Příloha 3: Procesní analýza - Příjem tísňového volání 112

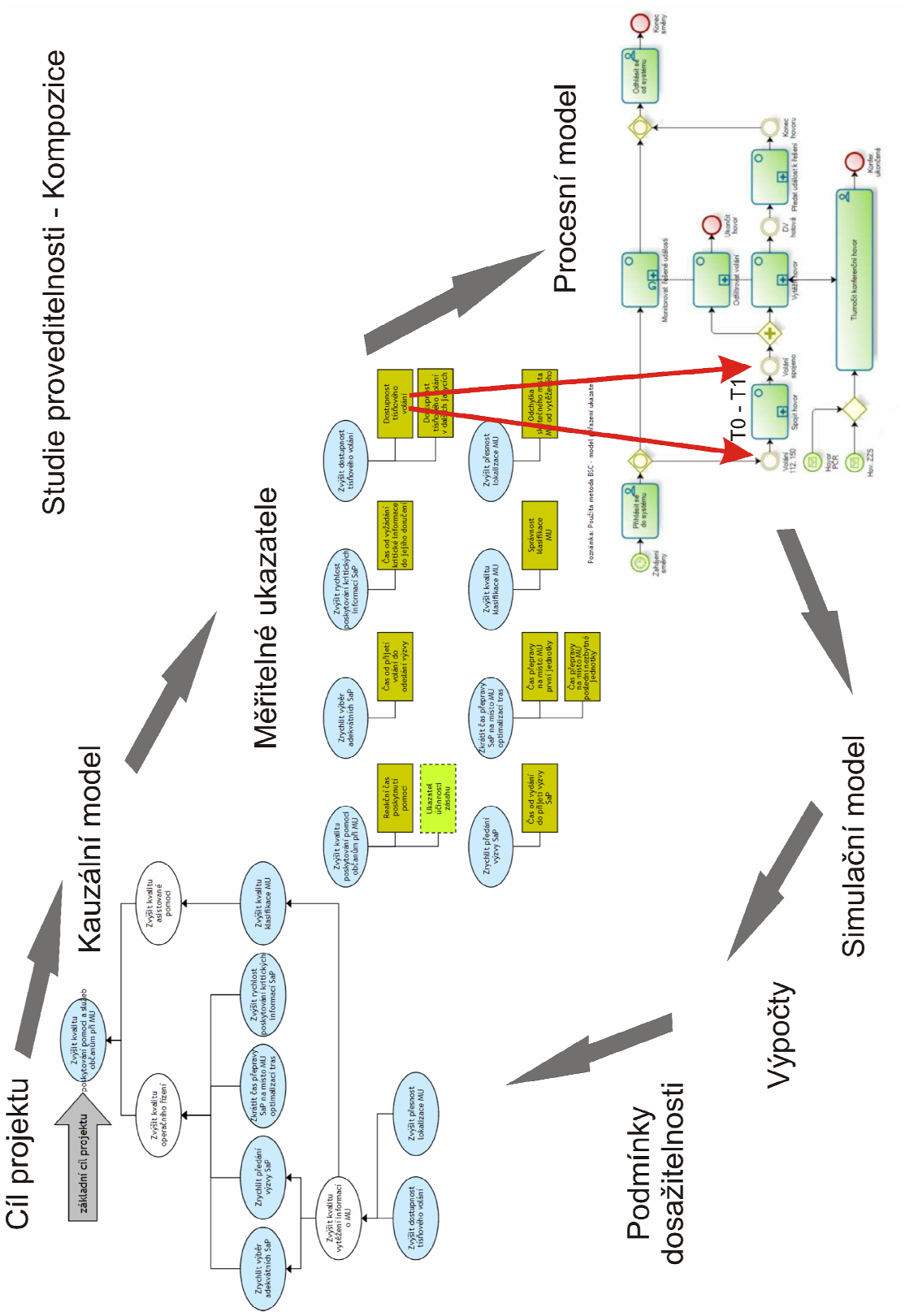
Příloha 4: Procesní analýza - Vyhodnocení komunikace složek IZS

Příloha 5: Procesní analýza - Operační řízení

14. Rejstřík

Přílohy:

Příloha 1



Příloha 2

Základní statistické údaje o činnosti JPO

Celkový přehled řešených událostí na území Jihomoravskéo kraje

III. čtvrtletí roku 2012

Typ události / Okres	JmK	Hodonín	Břeclav	Znojmo	Vyškov	Blansko	Brno-město	Brno-venkov
Požár (P) / Celkem	**452**	**72**	**48**	**33**	**29**	**36**	**152**	**82**
Požár	439	68	45	31	28	34	151	82
Požár bez účasti JPO	13	4	3	2	1	2	1	0
Dopravní nehoda (DN)	**464**	**45**	**50**	**39**	**50**	**61**	**88**	**131**
Dopravní nehoda silniční	437	42	47	37	49	58	84	120
Dopravní nehoda silniční hromadná	7	1	1	0	0	1	1	3
Dopravní nehoda železniční (vč. metra)	18	2	2	2	0	2	3	7
Dopravní nehoda letecká	0	0	0	0	0	0	0	0
Dopravní nehoda - ostatní	2	0	0	0	1	0	0	1
Únik nebezpečné chemické látky (UNL)	**111**	**5**	**12**	**5**	**9**	**9**	**54**	**17**
Únik plynu/aerosolu	30	1	4	0	2	1	19	3
Únik kapaliny (mimo ropných produktů)	8	0	0	0	0	2	4	2
Únik ropných produktů	67	4	6	5	5	6	31	10
Únik pevné látky	2	0	1	0	0	0	0	1
Únik nebezpečné chem. látky - ostatní	4	0	1	0	2	0	0	1
Technická havárie (TH)	**1 245**	**96**	**86**	**144**	**91**	**104**	**472**	**252**
Technická havárie	0	0	0	0	0	0	0	0
Technická pomoc	1 190	91	85	131	85	95	456	247
Technologická pomoc	3	0	0	0	0	0	2	1
Ostatní pomoc	52	5	1	13	6	9	14	4
Radiační havárie a nehoda	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
Ostatní mimořádné události	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
Planý poplach	**189**	**25**	**15**	**18**	**6**	**7**	**87**	**31**
	2 461	**243**	**211**	**239**	**185**	**217**	**853**	**513**

IV. čtvrtletí roku 2012

Typ události / Okres	JmK	Hodonín	Břeclav	Znojmo	Vyškov	Blansko	Brno-město	Brno-venkov
Požár (P) / Celkem	**294**	**25**	**24**	**22**	**29**	**18**	**116**	**50**
Požár	282	24	23	21	28	18	113	47
Požár bez účasti JPO	12	1	1	1	1	0	3	3
Dopravní nehoda (DN)	**437**	**43**	**52**	**45**	**50**	**52**	**87**	**115**
Dopravní nehoda silniční	411	34	50	43	49	47	82	112
Dopravní nehoda silniční hromadná	0	0	0	0	0	0	0	0
Dopravní nehoda železniční (vč. metra)	21	9	1	1	0	5	2	3
Dopravní nehoda letecká	0	0	0	0	0	0	0	0
Dopravní nehoda - ostatní	5	0	1	1	1	0	3	0
Únik nebezpečné chemické látky (UNL)	**102**	**6**	**6**	**5**	**9**	**13**	**52**	**9**
Únik plynu/aerosolu	36	2	1	1	2	2	23	4
Únik kapaliny (mimo ropných produktů)	4	0	0	0	0	1	3	0
Únik ropných produktů	56	4	5	3	5	10	22	4
Únik pevné látky	1	0	0	0	0	0	1	0
Únik nebezpečné chem. látky - ostatní	5	0	0	1	2	0	3	1
Technická havárie (TH)	**780**	**70**	**42**	**82**	**91**	**58**	**331**	**130**
Technická havárie	0	0	0	0	0	0	0	0
Technická pomoc	722	68	35	77	85	54	310	120
Technologická pomoc	9	0	0	0	0	0	4	5
Ostatní pomoc	49	2	7	5	6	4	17	5
Radiační havárie a nehoda	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
Ostatní mimořádné události	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
Planý poplach	**120**	**11**	**9**	**4**	**6**	**2**	**64**	**21**
	1 733	**155**	**133**	**158**	**185**	**143**	**650**	**325**

Příloha 3

Hasičský záchranný sbor ČR – příjem tísňového volání 112

Monitorovat řešené události

Problém: nejsou přenášeny stavy řešení událostí ze všech navazujících systémů

Není znám stav navazujících systémů

dispečer nemá přístup k detailu události založené mimo jeho TCTV

založené události se nacházejí na třech různých záložkách

Cíl: podat operátorovi přehledně aktuální informace o stavu řešení

Monitoring dostupnosti systémů

Technické řešení:

Zajistit komunikaci navazujících systémů (přenos stavů)

Provést úpravu aplikace – umožnit přístup k detailům všech událostí

Problém: monitoring provádí v současnosti manuálně obsluha

Cíl: efektivní automatické vyhodnocení potřebných informací

Technické řešení:

Nastavení automatických akcí (varování při neřešení)

Lokalizovat pomocí GIS

Problém: GIS v současnosti slouží pouze k pasivnímu zobrazování informací, neumožňuje interaktivní využité

Cíl: maximum informací zadávat přes GIS

Technické řešení:

Úprava GIS modulu, provázání jednotlivých mapových vrstev

Klasifikovat událost

Problém: nepřehledné číselníky součinnostních složek - v konečném důsledku používáno jen HZS

Cíl: stanovit jednoduché funkční číselníky

Stanovit vazby mezi číselníky složek

Předat událost k řešení

Problém: mnohdy není možné vytvořit telefonní spojení na OS součinnostních složek (nezvedají, obsazeno)

Cíl: zajistit garantovaný kanál pro předávání ze 112

Technické řešení:

Vyhrazená linka na předávání

Technologické řešení call-center, záložní směrování

Organizační řešení:

Vyčleněné pracoviště pro odbavení přepojených hovorů

Příloha 4

Vyhodnocení komunikace složek IZS

Nasadit SaP

Problém: příslušná obsluha KOPIS nedostává cíleně aktualizované informace v datové podobě upřesněné

- Zasahujícími SaP složek IZS
- operačními středisky PČR a ZZS, získanými z tísňových volání na linky 155 a 158

Cíl: průběžné dopřesňování informací o mimořádné události

Technické řešení:

Vzájemná informovanost operačních středisek o skutečnostech majících vliv na průběh řešení mimořádné události (příjem dat o mimořádné události, výjezd složky, složka na místě, odjezd složky z místa, ukončení řešené události – nutno specifikovat s jednotným výkladem).

Přehled o SaP složek IZS určených k řešení mimořádné události (první složka IZS, která přijíždí k místu události předává informaci o místě ostatním)

Vytěžit volání s podporou IS ZZS, PČR:

Problém:

- předávání informací vytěžených z tísňových volání na národní čísla 155 a 158 bývá zpožděno v důsledku prvotního nasazování svých sil a prostředků, poskytování rad a informací oznamovateli
- nastává také v případě, že tísňový hovor vytěžuje jeden dispečer a druhý, bez znalosti informací od oznamovatele, vyrozumívá další složky IZS

Cíl: získání validních informací pro všechny složky IZS určené k jejímu řešení bez prodlevy

Poskytování rad a informací ohlašovateli přechází do procesu operačního řízení, navýšení počtu obsluh na ZZS a PČR (daň za minimalizaci času potřebného k efektivnímu vyslání SaP všech složek IZS). Je nutné stanovit hranici, kdy musí rady a informace poskytovat operátor na příjmu a kdy operátor v procesu operačního řízení.

Technické řešení:

- Obsluhy tísňových linek 155 a 158 klasifikují v SW aplikaci tak, že jí v reálném čase (ještě v době hovoru a poskytování rad a informací ohlašovateli) sdílí s OD HZS a PČR v případě příjmu na 158 klasifikace IZS pro HZS a ZZS. Klasifikace pro IZS je prováděna v době kdy obsluha zjistí, že půjde o událost IZS.
- Stanovení nepodkročitelného minima informací, které musí obsahovat DV od jedné složky IZS k druhé. Tak aby bylo možné efektivní nasazení odpovídajících SaP složek IZS
- Zavedení oboustranné datové komunikace.

Organizační řešení:

- oddělení procesů příjmu a tísňového volání u ZZS
- Informace o přijímané události předává složkám IZS druhý operátor ZZS (stávající stav).

  Nevýhody: druhý operátor nepředává validní informace potřebné k efektivnímu nasazení odpovídajících SaP HZS a PČR. V případě příjmu na 158, odpovídajících SaP HZS a ZZS.

- Odborná příprava řešící potřeby všech složek IZS resp. jejich OPS

  Výhody: minimalizování zavlečení chyby v informacích k mimořádné události

Doporučení: kombinace technického a organizačního řešení

DV „bloudí“

Problém:

- zpoždění přenosu datových vět při rozsáhlých mimořádných událostech – přetížené datové cesty nebo výpadku datových cest
- DV byla předaná, ale z neznámých příčin nebylo zahájeno řešení události okamžitě

Příloha 5

Hasičský záchranný sbor ČR – operační řízení

Provést zkoušky technologie

Problém: zkoušky časově i akusticky zatěžují obsluhy KOPIS

Cíl: zkrácení času obsluhy KOPIS HZS kraje

Technické řešení (varianty – Externí /krajský):

- Externí dohled

  Výhody: nezatěžuje obsluhy KOPIS HZS kraje

  Nevýhody: finanční náklady rostou s rozsahem dohledovaných technologií

- Dohledový nástroj HZS kraje

  Výhody: nezatěžuje obsluhy KOPIS HZS kraje, tak jako fyzické zkoušky technologií

  Nevýhody: cena nástroje, zatížení obsluhy na vyhodnocení

Organizační řešení (varianty – centrálně / regionálně):

- Zajištění dohledu centrálně z GŘ HZS ČR

  Výhody: nezatěžuje obsluhy KOPIS HZS kraje, proaktivní dohled

  Nevýhody: odbornost a znalost regionálních technologií

- Zajištění dohledu regionálně

  Výhody: regionální znalost technologií, proaktivní dohled

  Nevýhody: nesystemizovaná místa techniků KIS na směnách KOPIS HZS kraje

Doporučení: kombinace technického a organizačního řešení

Provádění monitoringu situace

Problém: monitoring provádí v současnosti manuálně obsluha KOPIS

Cíl: efektivní automatické vyhodnocení potřebných informací

Technické řešení:

- Vizualizace monitorovaných oblastí monitoringu v GIS

  Výhody: jednotné prostředí pro vyhodnocení informací

  Nevýhody: zranitelnost

- Dynamické nastavení kritérií

  Výhody: obsluha KOPIS může nastavit kritéria pro upozornění na nestandardní stav

Doporučení: realizace technického řešení

Nasadit SaP

Problém:

- není zajištěný datový tok aktuálních dat spravovaných HZS, digitálních podob poplachových plánů atd. mezi všemi potřebnými uzly

Cíl: efektivní využití dostupných SaP

Technické řešení:

- Centrální databáze jednotek PO a techniky PO

  Výhody: realizace mezikrajskáých dohod na mezikrajskou výpomoc, aktuální stav sousedních SaP určených pro mezikrajskou výpomoc

  Nevýhody: finanční náklady na centrální databázi

- Implementace dat o SaP ostatních složek IZS do SW IS Výjezd

  Výhody: realizace smluvních vztahů z dohod

  Nevýhody: finanční náklady na implementaci

- Implementace dat o subjektech nasmlouvaných dle dohod IZS do SW IS Výjezd

Organizační řešení:

- Vyhodnocení potřebných dohod – ostatních složek IZS

  Výhody: uzavírání dohod se skutečně potřebnými složkami

  Nevýhody: nesystemizovaná místa analytiků u HZS krajů

Doporučení: realizace technického řešení, důsledkem bude výstup potřebných skutečně potřebných ostatních složek IZS.

Komunikace s jednotkami PO

Problém:

- informace o místě MU předávané jednotkám HZS krajů jen slovním popisem na příkazu k výjezdu
- extrémní zatížení hlasových komunikací z místa MU
- chybí informace o aktuální poloze jednotek v terénu

Cíl: zefektivní komunikace s jednotkami PO

Technické řešení:

- Důsledné využití dostupných, existujících funkcionalit systémů
  a. tisk mapy na PKV
  b. statusy, nasazení hovorových skupin pro komunikace v jednotném prostředí složek IZS
  c. navigace/sledování vozidel

Organizační řešení:

- Vyčlenění příslušníka/člena jeho v jednotce PO pro komunikaci s KOPIS HZS kraje

  Výhody: jednotné řešení u HZS ČR

  Nevýhody: oslabení výkonu služby

- Odborná příprava zaměřená na komunikace ve výkonu služby

  Výhody: unifikace návyků v komunikování v rámci HSZ ČR

  Nevýhody: absence odborností a reálných zkušenostní v učilištích HZS ČR

Doporučení: realizace technického a organizačního řešení