Zdravotně sociální fakulta
Faculty of Health and Social Sciences

Jihočeská univerzita v Českých Budějovicích
University of South Bohemia in České Budějovice

Ochrana zdravotnického operačního střediska ZZS Plzeňského kraje jako prvku kritické infrastruktury

BAKALÁŘSKÁ PRÁCE

Studijní program: OCHRANA OBYVATELSTVA

Autor: MUDr. Pavel Hrdlička

Vedoucí práce: MUDr. Josef Štorek, Ph.D.

České Budějovice 2017

Prohlášení

Prohlašuji, že svoji bakalářskou práci s názvem „Ochrana zdravotnického operačního střediska ZZS Plzeňského kraje jako prvku kritické infrastruktury“ jsem vypracoval samostatně pouze s použitím pramenů v seznamu citované literatury.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce, a to v nezkrácené podobě elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby bakalářské práce. Rovněž souhlasím s porovnáním textu mé bakalářské práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

V Českých Budějovicích dne 3. května 2017

……

Podpis

Poděkování

Moje poděkování patří celému IT úseku ZZS Plzeňského kraje, zejména Ing. Petru Jáchimovi a Jaroslavu Kondelíkovi, kteří mi byli kdykoliv nápomocni v problematice IT se zaměřením na vybavení našeho zdravotnického operačního střediska a jeho kybernetickou bezpečnost. Z externích spolupracovníků naší organizace v tomto ohledu pak patří můj dík zástupcům firmy PER4MANCE s.r.o., jmenovitě Ing. Jiřímu Koutnému, Ing. Janu Jarošovi a Bc. Petru Křížovi, MSc., s jejichž souhlasem jsou použity i některé obrázky týkající se kybernetické problematiky.

V rámci spolupráce na poli krizové připravenosti bych rád poděkoval útvaru krizového řízení naší organizace, zejména pak referentce pracoviště krizové připravenosti Ing. Denise-Charlotte Ralbovské, která mi byla svými poznatky a připomínkami nápomocna v rámci problematiky kritické infrastruktury a Plánu krizové připravenosti. Z externích spolupracovníků pak patří můj dík Františkovi Kheilovi, a to za cenné rady a poskytnuté materiály v oblasti BOZP a PO.

Závěrem bych chtěl poděkovat svému vedoucímu práce MUDr. Josefu Štorkovi, Ph.D., který při mně stál jako můj učitelem a rádce během mých prvních krůčků na poli krizové připravenosti ve zdravotnictví a s kterým na této problematice spolupracuji nepřetržitě již dlouhá léta.

Ochrana zdravotnického operačního střediska ZZS Plzeňského kraje jako prvku kritické infrastruktury

Abstrakt

Cílem bakalářské práce je posoudit stav ochrany prvku kritické infrastruktury, v tomto případě zdravotnického operačního střediska Zdravotnické záchranné služby Plzeňského kraje.

V ní se nejprve zaměříme na situace přímého ohrožení budovy na podkladě mimořádné události či krizové situace, které vycházejí z analýzy rizik. Tato analýza rizik je součástí Krizového plánu Plzeňského kraje, jehož zpracovatelem je Hasičský záchranný sbor Plzeňského kraje. Na podkladě místního šetření budou posouzena stávající opatření v kontextu s již existujícími dokumenty, tedy zejména se zpracovaným plánem krizové připravenosti. Tato nejpravděpodobnější „klasická rizika“ budou podrobněji rozvedena včetně pro některé tyto události následující evakuace.

Bakalářská práce se v další části cíleně zaměří na „novodobé hrozby“, a to zejména na narušení kybernetické bezpečnosti, s posouzením stávajícího stavu zálohování informačních systémů a vlastního zabezpečení, uchování a zálohování elektronických dat. Provedením analýzy současného hardwarového a softwarového vybavení zdravotnického operačního střediska a příslušné síťové infrastruktury budou identifikovány konfigurace jednotlivých prvků, jejich vzájemné vztahy a hlavně jejich zabezpečení. V případě zjištění nevyhovujícího stavu budou navržena příslušná nápravná opatření.

Přínosem této bakalářské práce bude zařazení výsledku šetření týkající se kybernetické bezpečnosti do současného plánu krizové připravenosti, který tuto problematiku zatím neobsahuje. Výsledky a závěry bakalářské práce tedy budou využity ke zvýšení krizové připravenosti Zdravotnické záchranné služby Plzeňského kraje, a to ve smyslu ochrany prvku kritické infrastruktury.

Klíčová slova: zdravotnická záchranná služba, zdravotnické operační středisko, prvek kritické infrastruktury, plán krizové připravenosti, kybernetická bezpečnost

Protecting the Health Operations Centre of Emergency Medical Services Pilsen Region as a Critical Infrastructure Element

Abstrakt

The aim of the bachelor thesis is to assess the conservation status of the critical infrastructure element, in this case medical operations centre of the Emergency Medical Service of the Pilsner region.

Firstly, the work deals with situations of the imminent danger of the building on the basis of emergency or crisis situations, which are based on the risk analysis. This risk analysis is a part of the Emergency Plan of the Pilsen Region, which has been prepared by the Fire Brigade of the Pilsner region. On the basis of local investigations there are evaluated some current measures in the context of already existing documents, namely the processed crises preparedness plan. These most probable "classic risks" are then further elaborated including evacuation as a typical measure for some of them.

In the next section this Bachelor thesis has focused on the "new threats", mainly on a violation of a cyber security, with an assessment of the current state of backup systems and their own security, storage and the backup of the electronic data. Analyzing the current hardware and software of the operating medical centres and related infrastructure network, there are identified configurations of some individual elements, their relationships and especially their security. Some remedial measures are suggested in case of the unsatisfactory situation.

The benefit of this work is the inclusion of results of the investigation related to cyber security in the current crisis preparedness plan, which has not included this issue yet. The results and conclusions of this bachelor thesis are therefore used to improve crisis preparedness of Emergency Medical Services of Pilsen region in terms of the protection of the critical infrastructure element.

Keywords: Emergency Medical Services, Health Operations Centre, a critical infrastructure element, an emergency preparedness plan, a cyber security

Obsah

Úvod **8**

1 Teoretická část **9**

1.1 Vysvětlení základních pojmů 9

1.2 Vymezení zdravotnické záchranné služby 11

1.3 Organizace zdravotnického zařízení poskytovatele ZZS 13

1.4 Organizace a základní úkoly ZOS 14

1.5 ZOS jako prvek kritické infrastruktury 14

1.6 Plán krizové připravenosti 17

1.7 Terorismus a kybernetická bezpečnost 18

2 Cíl práce a výzkumná otázka **21**

2.1 Cíl práce 21

2.2 Výzkumná otázka 21

3 Metodika **22**

4 Výsledky šetření a výzkumu **23**

4.1 ZZS Plzeňského kraje jako zvolený poskytovatel zdravotní služby 23

4.2 Kritéria pro stanovení nejpravděpodobnějších rizik daného prvku 24

4.3 Nejpravděpodobnější rizika v rámci klasických hrozeb 25

4.3.1 Výpadek dodávky energie *27*

4.3.2 Požár budovy *29*

4.3.3 Evakuace ZOS z důvodu hrozící MU *36*

4.3.4 Epidemie mezi zaměstnanci *39*

4.4 Nejpravděpodobnější rizika v rámci novodobých hrozeb 42

4.4.1 Popis infrastruktury ZOS *42*

4.4.2 Hardware *44*

4.4.3 Software *48*

4.4.4 Síťová infrastruktura *51*

4.4.5 Zabezpečení ... *53*

5 Diskuze ... **61**

5.1 Posouzení efektivnosti současných opatření ... 61

5.1.1 Výpadek dodávky energie ... *61*

5.1.2 Požár budovy, opatření PO ... *61*

5.1.3 Evakuace ZOS z důvodu hrozící MU ... *62*

5.1.4 Epidemie mezi zaměstnanci ... *62*

5.2 Posouzení kybernetické bezpečnosti, návrh na její doplnění ... 63

5.3 Odpověď na výzkumnou otázku ... 64

6 Závěr ... **65**

Seznam použitých zdrojů ... **66**

Seznam zkratek ... **70**

Seznam obrázků ... **77**

Seznam příloh ... **78**

Úvod

Obecně připravenost zdravotnické záchranné služby ve smyslu krizové připravenosti v rámci ochrany prvku kritické infrastruktury je elementárním předpokladem bezproblémového chodu záchranné služby a tím i zabezpečení její primární funkce, kterou je poskytování přednemocniční neodkladné péče (PNP).

Teoretická část je zaměřena na výklad základních pojmů s odkazem na právní prostředí řešící problematiku kritické infrastruktury na různých úrovních a obecně na určení a vlastní ochranu prvků této infrastruktury. Vlastní posouzení rizik pak vychází ze zpracovaného plánu krizové připravenosti (PKP) prvku – subjektu kritické infrastruktury pro zdravotnické operační středisko zdravotnické záchranné služby (ZOS ZZS), případně z krizového plánu kraje, jehož zpracovatelem je hasičský záchranný sbor (HZS) kraje.

Praktická část je zaměřena na posouzení stávající ochrany v kontextu se zpracovanými dokumenty (např. PKP) a platnými normami, nově pak s cíleným zaměřením na nové hrozby charakteru ohrožení kybernetické bezpečnosti včetně stavu zálohování informačních systémů, zabezpečení, uchování a zálohování elektronických dat. Vzhledem ke globálnímu nárůstu celosvětového terorismu a všeobecně nárůstu četnosti incidentů charakteru kybernetických útoků tato problematika neustále narůstá na své významnosti.

Na základě této provedené analýzy v korelaci se současným stavem budou v případě jeho nevyhovujícího stavu navrženy nápravná opatření ke zvýšení krizové připravenosti Zdravotnické záchranné služby Plzeňského kraje, a to ve smyslu vlastní ochrany prvku kritické infrastruktury, kterým je jeho zdravotnické operační středisko, tzv. „srdce“ záchranné služby.

1 Teoretická část

K porozumění problematiky je nezbytná orientace v základních pojmech. Základní právní normou řešící činnosti zdravotnické záchranné služby je **zákon č. 374/2011 Sb., o zdravotnické záchranné službě**, dále pak **zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách)** a v rámci havarijní či krizové připravenosti **zákony č. 239/2000 Sb., o integrovaném záchranném systému a o změně některých zákonů** a **č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů**.

1.1 Vysvětlení základních pojmů

- *„**Poskytovatelem zdravotních služeb** se rozumí fyzická nebo právnická osoba, která má oprávnění k poskytování zdravotních služeb podle tohoto zákona“*. (§ 2 odst. 1 zákona č. 372/2011 Sb.)

- Podle § 2 odst. 2 zákona č. 372/2011 Sb. se **zdravotními službami se rozumí***:*

  a) *„poskytování zdravotní péče podle tohoto zákona zdravotnickými pracovníky, a dále činnosti vykonávané jinými odbornými pracovníky, jsou-li tyto činnosti vykonávány v přímé souvislosti s poskytováním zdravotní péče,*
  b) *konzultační služby, jejichž účelem je posouzení individuálního léčebného postupu, popřípadě navržení jeho změny nebo doplnění, a další konzultace podporující rozhodování pacienta ve věci poskytnutí zdravotních služeb prováděné dalším poskytovatelem zdravotních služeb (dále jen „poskytovatel“) nebo zdravotnickým pracovníkem, kterého si pacient zvolil,*
  c) *nakládání s tělem zemřelého v rozsahu stanoveném tímto zákonem, včetně převozu těla zemřelého na patologicko-anatomickou pitvu nebo zdravotní pitvu a z patologicko-anatomické pitvy nebo ze zdravotní pitvy prováděné poskytovatelem podle zákona o pohřebnictví,*
  d) ***zdravotnická záchranná služba**,*
  e) *zdravotnická dopravní služba, jejímž účelem je*

1. *přeprava pacientů mezi poskytovateli nebo k poskytovateli a zpět do vlastního sociálního prostředí, je-li to nezbytné k zajištění poskytnutí zdravotních služeb,*
2. *rychlá přeprava zdravotnických pracovníků k zabezpečení neodkladné péče u poskytovatele,*
3. *přeprava osob včetně zemřelého pacienta související s prováděním transplantací, neodkladná přeprava tkání a buněk určených k použití u člověka, přeprava léčivých přípravků, krve a jejích složek a zdravotnických prostředků nezbytných pro poskytnutí neodkladné péče nebo přeprava dalšího biologického materiálu,*

f) přeprava pacientů neodkladné péče, kterou se rozumí jejich přeprava mezi poskytovateli výhradně za podmínek soustavného poskytování neodkladné péče během přepravy,

g) zdravotní služby v rozsahu činnosti odběrových zařízení nebo tkáňových zařízení podle jiných právních předpisů upravujících postupy pro zajištění jakosti a bezpečnosti lidských orgánů, tkání a buněk,

h) zdravotní služby v rozsahu činnosti zařízení transfuzní služby nebo krevní banky podle právního předpisu upravujícího výrobu transfuzních přípravků, jejich skladování a výdej.“

„Zdravotními službami se rovněž rozumí specifické zdravotní služby podle zákona o specifických zdravotních službách, zdravotní služby podle zákona upravujícího transplantace nebo zákona upravujícího umělé přerušení těhotenství.“ (§ 2 odst. 3 zákona č. 372/2011 Sb.)

- „***Zdravotní péčí*** *se rozumí:*

a) soubor činností a opatření prováděných u fyzických osob za účelem

1. *předcházení, odhalení a odstranění nemoci, vady nebo zdravotního stavu (dále jen „nemoc“),*
2. *udržení, obnovení nebo zlepšení zdravotního a funkčního stavu,*
3. *udržení a prodloužení života a zmírnění utrpení,*
4. *pomoci při reprodukci a porodu,*
5. *posuzování zdravotního stavu,*

b) *preventivní, diagnostické, léčebné, léčebně rehabilitační, ošetřovatelské nebo jiné zdravotní výkony prováděné zdravotnickými pracovníky (dále jen „zdravotní výkon“) za účelem podle písmene a).*“ (§ 2 odst. 4 zákona č. 372/2011 Sb.)

1.2 Vymezení zdravotnické záchranné služby

Základní ustanovení o zdravotnické záchranné službě jsou obsažena v jejím zákoně č. 374/2011 Sb., § 2 tohoto zákona uvádí:

*„**Zdravotnická záchranná služba** je zdravotní službou, v jejímž rámci je na základě tísňové výzvy, není-li dále stanoveno jinak, poskytována zejména přednemocniční neodkladná péče osobám se závažným postižením zdraví nebo v přímém ohrožení života. Součástí zdravotnické záchranné služby jsou další činnosti stanovené tímto zákonem.*“

Podle § 4 zákona č. 374/2011 Sb. **zahrnuje zdravotnická záchranná služba tyto činnosti**:

a) „nepřetržitý kvalifikovaný bezodkladný příjem volání na národní číslo tísňového volání 155 a výzev předaných operačním střediskem jiné základní složky integrovaného záchranného systému (dále jen „tísňové volání“) operátorem zdravotnického operačního střediska nebo pomocného operačního střediska,

b) vyhodnocování stupně naléhavosti tísňového volání, rozhodování o nejvhodnějším okamžitém řešení tísňové výzvy podle zdravotního stavu pacienta, rozhodování o vyslání výjezdové skupiny, rozhodování o přesměrování výjezdové skupiny a operační řízení výjezdových skupin,

c) řízení a organizaci přednemocniční neodkladné péče na místě události a spolupráci s velitelem zásahu složek integrovaného záchranného systému,

d) spolupráci s cílovým poskytovatelem akutní lůžkové péče,

e) poskytování instrukcí k zajištění první pomoci prostřednictvím sítě elektronických komunikací v případě, že je nezbytné poskytnout první pomoc do příjezdu výjezdové skupiny na místo události,

f) vyšetření pacienta a poskytnutí zdravotní péče, včetně případných neodkladných výkonů k záchraně života, provedené na místě události, které směřují k obnovení nebo stabilizaci základních životních funkcí pacienta,

g) soustavnou zdravotní péči a nepřetržité sledování ukazatelů základních životních funkcí pacienta během jeho přepravy k cílovému poskytovateli akutní lůžkové péče, a to až do okamžiku osobního předání pacienta zdravotnickému pracovníkovi cílového poskytovatele akutní lůžkové péče,

h) přepravu pacienta letadlem mezi poskytovateli akutní lůžkové péče za podmínek soustavného poskytování neodkladné péče během přepravy, hrozí-li nebezpečí z prodlení a nelze-li přepravu zajistit jinak,

i) přepravu tkání a orgánů k transplantaci letadlem, hrozí-li nebezpečí z prodlení a nelze-li přepravu zajistit jinak,

j) *třídění osob postižených na zdraví podle odborných hledisek urgentní medicíny při hromadném postižení osob v důsledku mimořádných událostí nebo krizových situací.*“

Zdravotnická záchranná služba *jako „základní složka integrovaného záchranného systému zajišťuje nepřetržitou pohotovost pro příjem ohlášení vzniku mimořádné události, její vyhodnocení a neodkladný zásah v místě mimořádné události. Za tímto účelem rozmísťují své síly a prostředky po celém území České republiky.*“ (§ 4 odst. 4 zákona č. 239/2000 Sb.)

Činnosti k připravenosti poskytovatele zdravotnické záchranné služby na řešení mimořádných událostí definuje § 20 zákona č. 374/2011 Sb.:

(1) „Činnostmi k připravenosti poskytovatele zdravotnické záchranné služby na řešení mimořádných událostí a krizových situací jsou činnosti, kterými jsou zajišťovány úkoly

a) k přípravě na řešení mimořádných událostí a krizových situací pro oblast poskytování zdravotnické záchranné služby,

b) k přípravě na společné zásahy složek integrovaného záchranného systému,

c) vyplývající z dokumentace integrovaného záchranného systému.

(2) Poskytovatel zdravotnické záchranné služby je povinen

a) nepřetržitě zajišťovat činnosti k připravenosti na mimořádné události a krizové situace,

b) zpracovat podklady k dokumentaci integrovaného záchranného systému.

(3) *Činnosti k připravenosti na řešení mimořádných událostí a krizových situací zajišťuje poskytovatel zdravotnické záchranné služby prostřednictvím pracoviště krizové připravenosti. Úkoly pro zajištění činností k připravenosti na řešení mimořádných událostí a krizových situací je poskytovatel zdravotnické záchranné služby povinen plnit podle postupů stanovených v rámci plánovacích dokumentů orgánů krizového řízení, havarijního plánování a dokumentace integrovaného záchranného systému*.“

Tyto činnosti zdravotnické složky v místě mimořádné události s hromadným postižením osob (MU s HPO) dále stanovuje a rozpracovává vyhláška č. 240/2011 Sb., kterou se provádí zákon o zdravotnické záchranné službě, a to ve svých §§ 6–11.

1.3 Organizace zdravotnického zařízení poskytovatele ZZS

Organizaci zdravotnického zařízení poskytovatele ZZS stanovuje opět zákon o zdravotnické záchranné službě, který uvádí ve svém § 9:

(1) „Zdravotnickým zařízením poskytovatele zdravotnické záchranné služby se rozumí prostory a mobilní prostředky určené pro poskytování zdravotnické záchranné služby (dále jen „zařízení zdravotnické záchranné služby“).

(2) Zařízení zdravotnické záchranné služby vždy tvoří

a) ředitelství,

*b) **zdravotnické operační středisko**,*

c) výjezdové základny s výjezdovými skupinami,

d) pracoviště krizové připravenosti,

e) vzdělávací a výcvikové středisko.

(3) Součástí zařízení zdravotnické záchranné služby jsou i pomocná operační střediska a pracoviště pro poskytování jiných zdravotních služeb, jsou-li zřízena.“

1.4 Organizace a základní úkoly ZOS

Organizační členění a úkoly zdravotnického operačního střediska nám stanovuje zákon o ZZS ve svém § 11 následovně:

(1) „Zdravotnické operační středisko je centrálním pracovištěm operačního řízení, které pracuje v nepřetržitém režimu.

(2) Operačním řízením se pro účely tohoto zákona rozumí zejména

a) příjem a vyhodnocení tísňových volání,

b) převzetí a vyhodnocení výzev a vyrozumění přijatých od základních složek integrovaného záchranného systému a od orgánů krizového řízení,

c) vydávání pokynů výjezdovým skupinám na základě přijatých tísňových výzev,

d) poskytování instrukcí k zajištění první pomoci prostřednictvím sítě elektronických komunikací, je-li nezbytné poskytnout první pomoc do příjezdu výjezdové skupiny na místo události,

e) spolupráce s ostatními zdravotnickými operačními středisky, pomocnými operačními středisky a operačními a informačními středisky integrovaného záchranného systému,

f) koordinace činnosti pomocných operačních středisek,

g) zajišťování komunikace mezi poskytovatelem zdravotnické záchranné služby a poskytovateli akutní lůžkové péče,

h) koordinace předávání pacientů cílovým poskytovatelům akutní lůžkové péče,

i) koordinace přepravy pacientů neodkladné péče mezi poskytovateli zdravotních služeb podle zákona o zdravotních službách.“

Dále pak již dříve zmíněná vyhláška č. 240/2012 Sb. nám ve svém § 4 upřesňuje obsah **organizačně provozního řádu zdravotnického operačního střediska**.

1.5 ZOS jako prvek kritické infrastruktury

Definice kritické infrastruktury, resp. prvku kritické infrastruktury, jejich význam a znění vychází jak z legislativy evropské (unijní), tak z naší národní.

Dne 8. prosince 2008 v úředním věstníku Evropské unie částky L 345/75-82 vychází **směrnice Rady 2008/114/ES o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu**, kde definicí kritické infrastruktury (KI) se rozumí *„prostředky, systémy a jejich části nacházející se v členském státě, které jsou zásadní pro zachování nejdůležitějších společenských funkcí, zdraví, bezpečnosti, zabezpečení nebo dobrých hospodářských či sociálních podmínek obyvatel a jejichž narušení nebo zničení by mělo pro členský stát závažný dopad v důsledku selhání těchto funkcí*“. (čl. 2 písm. a) směrnice Rady 2008/114/ES)

Naše národní právní norma nám pak definuje v krizovém zákoně **jako kritickou infrastrukturou** *„prvek KI nebo systém prvků KI, jehož narušení funkce by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu.“* (§ 2 písm. g) zákona č. 240/2000 Sb.)

Dále pak ve stejném § téhož zákona **jako prvek KI** *„zejména stavbu, zařízení, prostředek nebo veřejnou infrastrukturu, určenou podle průřezových a odvětvových kritérií; je-li prvek kritické infrastruktury součástí evropské kritické infrastruktury, považuje se za prvek evropské kritické infrastruktury*“. (§ 2 písm. i) zákona č. 240/2000 Sb.)

Výše zmíněná odvětvová a průřezová kritéria nám stanovuje další právní předpis, a to **nařízení vlády č. 432 ze dne 22. prosince 2010, o kritériích pro určení prvku kritické infrastruktury**, kde vláda nařizuje podle § 40 odst. 1 zákona č. 240/2000 Sb., ve znění zákona č. 320/2002 Sb., o změně a zrušení některých zákonů v souvislosti s ukončením činnosti okresních úřadů a zákona č. 430/2010 Sb., kterým se mění zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů, k provedení § 4 odst. 1 písm. d) tohoto zákona:

- **průřezová kritéria** (§ 1 NV č. 432/2010 Sb.)

Průřezovým kritériem pro určení prvku kritické infrastruktury je hledisko

a) obětí s mezní hodnotou více než 250 mrtvých nebo více než 2 500 osob s následnou hospitalizací po dobu delší než 24 hodin,
b) ekonomického dopadu s mezní hodnotou hospodářské ztráty státu vyšší než 0,5 % hrubého domácího produktu, nebo

c) **dopadu na veřejnost s mezní hodnotou rozsáhlého omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího více než 125 000 osob.**

- **odvětvová kritéria** (§ 2 a příloha NV č. 432/2010 Sb.)

Odvětvová kritéria pro určení prvku kritické infrastruktury jsou uvedena v příloze k tomuto nařízení. Z nich jsou následně vyjmuta jen 2, a to:

IV. ZDRAVOTNICTVÍ

Zdravotnické zařízení, jehož celkový počet akutních lůžek je nejméně 2 500.

VIII. NOUZOVÉ SLUŽBY

A. integrovaný záchranný systém (IZS)

a) operační a informační středisko generálního ředitelství Hasičského záchranného sboru České republiky,
b) operační a informační středisko hasičského záchranného sboru kraje,
c) stanice Hasičského záchranného sboru České republiky,
d) operační středisko útvaru Policie České republiky,
e) **operační středisko zdravotnické záchranné služby**,
f) centrální a oblastní dispečinky horské služby.

Z výše uvedeného tedy vyplývá, že ZZS, resp. jeho ZOS vyhovuje jak průřezovému kritériu uvedeným pod písmenem c), tak odvětvovému kritériu – nikoliv pro oblast zdravotnictví, ale pro nouzové služby, resp. IZS.

Dne 11. června 2012 Ministerstvo vnitra České republiky (MV ČR) jako příslušný ústřední správní úřad vydává **dokument pod čj. MV-55222-2/PO-OKR-2012 jako opatření obecné povahy (OOP)**, které ***určuje*** ve smyslu § 9 odst. 3 písm. c) zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů, nařízení vlády č. 432/2010 Sb. o kritériích pro určení prvku kritické infrastruktury, a v souladu s ustanovením § 171 zákona č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů, ***prvky kritické infrastruktury, jejichž provozovatelem není organizační složka státu v odvětví „nouzové služby“ na území České republiky***.

Za provozovatele prvku KI ustanovuje tímto OOP jako gestor odvětví „nouzové služby“ MV ČR **„Zdravotnickou záchrannou službu Plzeňského kraje (ZZS PK)“** a určuje jako prvek KI její **„krajské zdravotnické operační středisko“**.

1.6 Plán krizové připravenosti

V souladu s ustanovením § 14 odst. 2 písm. c) zákona č. 240/2000 Sb. byl s účinností od 1. ledna 2013 schválen nový **Krizový plán Plzeňského kraje**.

Tento krizový plán (KP) byl zpracován Hasičským záchranným sborem Plzeňského kraje (HZS PK) v součinnosti s Krajským úřadem Plzeňského kraje (KÚ PK) a dalšímu dotčenými subjekty. Zpracovatelem KP byla ZZS PK zahrnuta do KP z hlediska zajištění plnění následujícího opatření vyplývajícího z KP, a to „zajištění přednemocniční neodkladné péče“. Na základě této skutečnosti byla ZZS PK, jako právnická osoba, která zajišťuje plnění opatření vyplývající z KP, povinna zpracovat dle § 29 odst. 1) krizového zákona **„plán krizové připravenosti“**.

Vzhledem k tomu, že ZZS PK, resp. jeho krajské ZOS bylo určeno MZ ČR prvkem kritické infrastruktury (PKI), může být **plán krizové připravenosti subjektu kritické infrastruktury** a **plán krizové připravenosti** sloučen do jednoho dokumentu. Tento zpracovaný dokument musí obsahovat náležitosti obou plánů (čl. 22, odst. 5 Metodiky zpracování plánů krizové připravenosti).

Obsah PKP je uveden v ustanovení § 17 nařízení vlády č. 462/2000 Sb., k provedení § 27 odst. 8 a § 28 odst. 5 zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), a při jeho tvorbě byla využita uvedená **„Metodika zpracování plánů krizové připravenosti“** podle §§ 17–18 výše zmíněného nařízení vlády. Tato metodika byla zpracována v gesci Ministerstva vnitra – Generálního ředitelství Hasičského záchranného sboru České republiky (MV – GŘ HZS ČR).

Vlastní způsob zpracování PKI byl podle § 18 odst. 1) nařízení vlády č. 462/2000 Sb. před jeho uveřejněním, resp. uvedením v platnost v rámci vnitropodnikových předpisů, projednán s příslušným orgánem krizového řízení.

1.7 Terorismus a kybernetická bezpečnost

Mezi novodobá rizika lze jistě řadit i terorismus. Jeho dřívější podoby v minulosti, v 19. či 20. století, byly činy spíše lokálního významu, charakteristické svým fundamentalismem či nacionalismem. Terorismus byl typický tím, že teroristé *„slepě a bezohledně útočí na civilní obyvatelstvo“*. (EICHLER, 2010)

Novodobý terorismus 21. století, resp. **3. tisíciletí** je již globálního charakteru, zasahující a napadající hodnoty civilizovaného světa kdekoliv. Navíc do pole strategie vstupuje nový „silný hráč“, kterým je **internet**, který je nejen využíván pro přenos informací, ale také desinformací, k šíření náboženské nenávisti, hlásání své „pravdy a idejí“, následně vyvolání strachu z krutosti ve formě záznamů z poprav zajatců. Internet slouží i k rekrutování nových členů a stoupenců např. Islámského státu, dále k aktivaci tzv. „spících buněk“, kdy tito stoupenci teroristických skupin naplánují své činy, a pak přímo útočí v cílových zemích jejich zájmu.

Zcela novým, nikoliv ale méně důležitým fenoménem je **tzv. kybernetická bezpečnost**. Dnešní civilizovaná společnost má svoje hodnoty a vlastní infrastrukturu postavenu na využití elektrické energie a nejnovějších informačních technologií (IT). Bez světa digitalizace, počítačů či internetu si svůj život dokáže už jen málokdo představit. Budoucností je pak vývoj umělé inteligence k využití plné automatizace či robotizace procesů.

Tedy při prolomení kybernetické bezpečnosti lze cíleným útokem buď ekonomicky poškodit daný subjekt (stát), ovlivnit jeho procesy šířením informací, resp. někdy účinněji desinformací s vyvoláním chaosu, nebo zcela vyřadit jeho infrastrukturu, a to dokonce i tu určenou k vlastní ochraně či obraně a nabourávající tak suverenitu a bezpečnost státu.

Hackerské útoky jsou čím dál tím sofistikovanější a tedy i nebezpečnější. Příkladem budiž v poslední době zprávy o možném ovlivnění výsledků letošních voleb v USA, Francii či Holandsku, kdy podezření v tomto případě padá na heckry ze zemí bývalého Sovětského svazu, resp. současného Ruska, navíc podporované z „horních pater“ současného governmentu.

„Skandály“ toho typu se bohužel již nevyhýbají ani samotné České republice, a to opět na nejvyšší úrovni státní správy. V lednu t. r. vydalo Ministerstvo zahraničních věcí České republiky (MZV ČR) tiskovou zprávu, kde přiznalo opakované několik měsíců trvající kybernetické útoky na vnější komunikační systém MZV, tedy na e-mailové schránky pracovníků úřadu, i jeho vedení. Vnitřní komunikační systém údajně narušen nebyl, a tedy nedošlo ani k úniku utajovaných informací. Jakmile kybernetičtí experti MZV zmíněný kybernetický útok zaznamenali, byly informovány jak Národní bezpečnostní úřad (NBÚ), resp. Národní centrum kybernetické bezpečnosti (NCKB), tak samotná vláda v čele s premiérem Bohuslavem Sobotkou a další zainteresovaní subjekty. (TS MZV ČR, 2017)

V rámci naplňovaní **zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)**, dále **ZKB**, a **vyhlášky NBÚ č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti), kterou se provádí zákon č. 181/2014 Sb. o kybernetické bezpečnosti**, dále jen **VKB,** a zároveň stanovení potřebné ochrany určených prvků KI byly osloveny NBÚ – NCKB i všechny krajské zdravotnické záchranné služby. Přípravná jednání pak vyvrcholila 12. ledna 2016 osobním setkáním zástupců jednotlivých ZZS (většinou ve složení na úrovni ředitelů, tedy statutárních zástupců, a IT specialistů těchto organizací) s experty NCKB na půdě NBÚ Na Popelce 2/16, Praha 5.

Hlavním cílem jednání bylo posouzení, zda informační a komunikační systémy (IS/KS), které jsou ve správě ZZS, naplňují kritéria stanovená pro kritické informační infrastruktury (KII) a posuzování významných informačních systémů (VIS). Určitým vodítkem byla **metodická příručka se základními informacemi a průvodcem pro určování KII / VIS vydaná NBÚ, resp. jeho NCKB** (verze 3 z 5. 8. 2015).

Tato metodická příručka je určena potenciálním povinným subjektům podle ZKB před prvním jednáním s NBÚ – NCKB ohledně určování prvků KII a posuzování VIS. Tento materiál má za cíl zmíněné procesy přiblížit a odpovědět na časté dotazy nejen u popisu procesu určování KII či VIS.

Na základě hromadné diskuze všech zúčastněných a prověření naplnění kritérií stanovených pro KII nařízením vlády č. 432/2010 Sb., bylo shledáno, byť ne 100%

názorem, ale většinovým, že **žádný ze systémů využívaných k činnosti ZZS v současné chvíli, resp. v dané době, a za současných podmínek kritéria pro prvky KII nenaplní.**

Tímto závěrem a přijatým usnesením se záchranné služby nemohly zapojit jako žadatelé o čerpání finančních prostředků z **integrovaného regionálního operačního programu (iROP), a to z výzvy č. 10 pro kybernetickou bezpečnost**.

Hlavní podporovanou aktivitou této 10. výzvy iROPu je zabezpečení tzv. VIS a KII veřejné správy dle ZKB, které zahrnuje následující kategorie:

- **fyzickou bezpečnost;**
- **ochranu integrity komunikačních sítí;**
- **ověřování identity uživatelů;**
- **řízení přístupových oprávnění;**
- **ochranu před škodlivým kódem;**
- **zaznamenávání činnosti KII a VIS, jejich uživatelů a administrátorů;**
- **detekci kybernetických bezpečnostních událostí;**
- **sběr a vyhodnocení kybernetických bezpečnostních událostí;**
- **aplikační bezpečnost;**
- **kryptografické prostředky;**
- **zajišťování úrovně dostupnosti informací;**
- **bezpečnost průmyslových a řídicích systémů**.

Finanční kritéria byla stanovena jako minimální dotace ve výši 3 mil. Kč s DPH a maximální dotace do 300 mil. Kč s DPH na jeden projekt. Termín podání žádostí končí k 30. 6. 2017.

2 Cíl práce a výzkumná otázka

2.1 Cíl práce

Cílem bakalářské práce je posoudit stav ochrany prvku kritické infrastruktury, v tomto případě zdravotnického operačního střediska ZZS Plzeňského kraje, a to jak po stránce přímého ohrožení budovy na podkladě mimořádné události či krizové situace vycházejícího z doposud zpracovaného **plánu krizové připravenosti**, resp. **plánu krizové připravenosti prvku (subjektu) kritické infrastruktury**, tak s cíleným zaměřením na nové hrozby v rámci kybernetické bezpečnosti včetně stavu zálohování informačních systémů a vlastního zabezpečení, uchování a zálohování dat.

2.2 Výzkumná otázka

Při vlastním šetření se bude bakalářská práce zabývat výzkumnou otázkou: „Jaký je současný stav krizové připravenosti, resp. ochrany prvku kritické infrastruktury – zdravotnického operačního střediska?„

3 Metodika

Teoretická část se zaměřuje nejprve na výklad pojmů, vycházejíce z dosavadních právních norem určujících činnost ZZS a jejího ZOS, následně navazuje na problematiku kritické infrastruktury – rešerši právních norem a dokumentů řešících problematiku kritické infrastruktury na různých úrovních a obecně na určení a vlastní ochranu prvků této kritické infrastruktury a nutné zpracování dokumentů, které vyplývá z dalších příslušných právních norem.

Následující praktická část se zabývá na podkladě místního šetření posouzením stávající ochrany v kontextu s již zpracovanými dokumenty, zejména s plánem krizové připravenosti. Vzhledem ke stanovenému rozsahu bakalářské práce nebude ale možné rozvést všechna tzv. „klasická rizika“, ale jen ta nejpravděpodobnější. Všechna rizika, resp. jejich výčet, preventivní opatření zabraňující vzniku dané MU, popř. reakce na ně pokud již nastanou a které slouží ke zmírnění jejich dopadu na chod a tedy vlastní funkci daného prvku KI, jsou právě předmětem dosavadně zpracovaného PKP.

Nejpravděpodobnější klasická rizika, resp. MU z nich potenciálně vzniklé, budou systematicky rozebrána podle následujícího klíče:

- **Popis MU.**
- **Příčina MU.**
- **Následky MU.**
- **Stávající ochranná opatření.**
- **Posouzení efektivnosti těchto opatření, event. návrh na doplnění dalšími** – tento bod bude již součástí navazující diskuze.

Praktická část zároveň identifikuje a doplňuje jejich výčet i o případná rizika nová, tedy o **tzv. „novodobé hrozby“**, která nejsou ještě v PKP zpracována. Nejprve je provedena analýza vybavení ZOS (hardware a software, síťová infrastruktura a vazby jednotlivých prvků) a jeho zabezpečení. Na jejím základě v korelaci se současnými trendy
a doporučeními je v případě nevyhovující stavu navrženo jejich doplnění do PKP s přijetím následných ochranných opatření.

4 Výsledky šetření a výzkumu

Na počátku vlastního šetření je nejprve upřesněn, resp. přiblížen subjekt, který bude cílem následujícího výzkumu. Taxativním vyjmenováním jsou uvedeny všechny subjekty v Plzeňském kraji poskytující na tomto území PNP. Další kapitoly jsou již věnovány danému prvku kritické infrastruktury, v tomto případě zdravotnickému operačnímu středisku.

4.1 ZZS Plzeňského kraje jako zvolený poskytovatel zdravotní služby

Daným kritériím uvedeným v teoretické části zcela vyhovuje a zároveň cílem výzkumu bude subjekt zajišťující přednemocniční neodkladnou péči, a to Zdravotnická záchranná služba Plzeňského kraje. V praktické části pak posoudíme připravenost, resp. ochranu jejího prvku kritické infrastruktury, kterým je zdravotnické operační středisko.

Zdravotnická záchranná služba Plzeňského kraje, která je příspěvkovou organizací Plzeňského kraje, vznikla 1. května. 2003 jako nástupnická organizace bývalého Územního střediska záchranné služby (ÚSZS) Plzeň se sídlem tř. E. Beneše 19, a to zřizovací listinou Zdravotnické záchranné služby Plzeňského kraje ze dne 15. dubna 2003, zapsanou v obchodním rejstříku u Krajského soudu v Plzni, pod spisovou zn. Pr 684.

V roce 2013 došlo k přestěhování ředitelství organizace, zároveň s výjezdovou základnou Plzeň-Bory, a to na současnou adresu Klatovská třída 2960/200i v Plzni do prostor nové budovy (*obrázek 1*) vystavěné v areálu bývalých kasáren nad plzeňskou věznicí na Borech. ZOS bylo na výše uvedenou novou adresu přesunuto až o rok později, tedy v roce 2014 a nachází se v 2. nadzemním podlaží budovy.

Dalším významným subjektem v rámci poskytování PNP v Plzeňském kraji je spolupracující provozovatel letecké záchranné služby (LZS), a tím je Armáda České republiky (AČR), jejíž působnost přesahuje rámec Plzeňského kraje. Dřívější ***Centrum letecké záchranné služby (CLZS)*** bylo v roce 2016 přejmenováno na ***Odbor letecké***

záchranné služby a urgentní medicíny AČR VZ 684810 se sídlem v Líních (obec nedaleko krajského města Plzeň).

Obrázek 1 – Budova ředitelství, ZOS a VZ Plzeň-Bory (zdroj: archív ZZS PK)

4.2 Kritéria pro stanovení nejpravděpodobnějších rizik daného prvku

Ke stanovení nejpravděpodobnějších rizik ve vztahu ke zvolenému prvku kritické infrastruktury nám poslouží následující kritéria:

- Územní příslušnost.
- Znalost organizační struktury ZZS PK.
- Znalost personálního a technického vybavení daného prvku, včetně informačních a komunikačních technologií (ICT).
- Znalost jednotlivých funkcionalit, jejich propojení a návaznost či závislost na sobě, tzn. síťová infrastruktura ZOS včetně informačních toků jak uvnitř, tak směrem ven mimo daný prvek.
- Specifikace rizikových míst těchto prvků infrastruktury – jejich funkcionalit či vzájemné interface, a to i z pohledu ve vztahu k příslušným stupňům řízení (na taktické, operační či strategické úrovni).

- Znalost MU či KS, které v minulosti již nastaly.

Za využití těchto výše definovaných základních kritérií bude vycházeno z poskytnuté zpracované dokumentace včetně výpočtů a nákresů, dále z vlastního místního šetření a posouzení reálné situace při znalosti všech funkcí ZOS, kdy budou následně stanovena nejpravděpodobnější rizika, ať z klasického či novodobého pojetí.

4.3 Nejpravděpodobnější rizika v rámci klasických hrozeb

Nejprve se zaměříme na nejčastější „klasická rizika“, zcela běžná v rámci 20. či 21. století. Mezi ně jistě patří **výpadek dodávky elektrického proudu** a **požár v prostorech budovy**.

Součástí života civilizované společnosti jsou pak i negativní jevy jako např. zneužívání tísňové linky či vyhrožování charakteru oznámení o **umístění nástražního výbušného systému v prostorách budov** (soudů, škol a dalších institucí) za účelem narušení jejich chodu. Často se jedná o „klukovinu“, kdy se děti či dospívající mládež snaží vyhnout např. svým povinnostem ve škole. Tento jev ale nelze tolerovat z důvodu své společenské nebezpečnosti, kdy od fáze fiktivní hrozby do fáze skutečné hrozby může být v 21. století v rámci rozvíjejícího se terorismu opravdu jen krůček. Tímto způsobem může být „ohroženo“ i operační středisko záchranné služby. Podcenění takové hrozby s následným vznikem MU, by jistě znamenalo kolaps zdravotnické záchranné služby s narušením její základní funkce. Pokud by zároveň byla na jiném místě kraje úmyslně vyvolána jiná MU s HPO, zejména dalším teroristickým činem, pak by výsledkem těchto dvou souběžných událostí byla pravděpodobně větší ztráta na životech občanů, anebo by to minimálně vedlo k významnému poškození jejich zdraví s šířením strachu a paniky.

Ve všech případech, kdy je nutná ***evakuace budovy***, v níž se nachází ZOS ZZS, je standardním postupem ke zmírnění dopadu MU na chod této KI plné zprovoznění ***pomocného*** či dočasné zprovoznění ***záložního operačního střediska***. Celý algoritmus je popsán ve zpracovaném **plánu krizové připravenosti**.

Poslední uvedenou nejpravděpodobnější hrozbou, která může postihnout chod ZOS, se jeví možná **epidemie**. Od dob poslední pandemie tzv. Hongkongské chřipky z let

1968–69 se celý svět připravuje při zákonitostech cyklického výskytu na novodobou vlnu této infekční nemoci. Určitou předzvěstí a varovně zdviženým prstem byla Mexická (prasečí) chřipka v roce 2009 a také nejznámější a nejsledovanější typ ptačí chřipky z přelomu 2. a 3. tisíciletí, kterým byl typ (kmen) tohoto viru H5N1. V letošním roce dochází opět k renesanci jejího výskytu, a to i v ČR. Naštěstí u tohoto kmene H5N8 nebyl prozatím nikde ve světě zaznamenán přenos z ptáků na člověka. (TS MZ ČR, 2017)

Epidemie, resp. pandemie nám však nehrozí jen ze strany viru chřipky, ale určitý potenciál skýtají i další infekční agens jako je tomu např. u koronarovirů. V nedávné době jsme mohli zaznamenat SARS (*Severe Acute Respiratory Syndrome*, neboli těžký akutní respirační syndrom či také syndrom náhlého selhání dýchání) – virové onemocnění dýchacích cest způsobené koronarovirem SARS-CoV a MERS (*Middle East Respiratory Syndrome)* - virové onemocnění dýchacích cest způsobené koronarovirem MERS-CoV, který způsobí selhání ledvin a plic.

Zde je přehled nejpravděpodobnějších rizik v rámci **„klasických hrozeb“**:

- **Výpadek dodávky elektrické energie**, ať lokálního charakteru, tak globálního pod pojmem „**black out**“.
- **Požár budovy či přímo na pracovišti ZOS** s následnou evakuací zaměstnanců.
- **Evakuace ZOS z různých dalších příčin, např. nahlášení údajného umístění nástražního výbušného systému** v prostorách operačního střediska.
- **Epidemie mezi zaměstnanci.**

4.3.1 Výpadek dodávky energie

Tato situace je prakticky nejčastější MU, která v organizaci nastává v nepravidelných časových intervalech. Z tohoto důvodu jí s nadsázkou už nelze považovat za „mimořádnou událost“, ale za „běžnou situaci“, kdy při přetížení distribuční sítě či její poruše nebo při plánované revizní odstávce dojde k náhlému či plánovanému přerušení dodávky el. proudu.

Mimořádnou událostí by se jistě tyto výpadky staly, pokud by organizace, resp. ZOS nebyla připravena či by výpadek el. proudu byl rozsáhlý a dlouhodobý charakteru „black-out“.

- **Popis MU**

Při výpadku elektrické energie dojde k přerušení dodávky el. proudu.

- **Příčina MU**

K výpadku el. proudu může dojí v rámci posuzované budovy buď závadou v elektroinstalaci, při poruše některého hlavního rozvaděče, ale také antropogenní činností, kdy nedbalostně, např. při vrtání do zdi, se může poškodit některý z důležitých hlavních rozvodů či jednotlivých kabelů. Mimo budovu pak může tato situace nastat při výkopových pracích, při níž může dojít k překopnutí podzemního vedení, a to nejen elektrického, ale i datového (optického kabelu), lžící bagru.

- **Následky MU**

Jednoznačným následkem by bylo narušení základní funkce ZOS, a to přijímání, vyhodnocování a následní předávání tísňových výzev výjezdovým skupinám. Na elektrickém proudu jsou plně závislé všechny zásadní technologie pro operační řízení. Tato situace by jistě v globále znamenala zhroucení tohoto prvku kritické infrastruktury.

- **Stávající opatření**

Aby bylo eliminováno ohrožení touto mimořádnou událostí, nachází se v suterénu budovy dieselový agregát (*obrázek 2*) pro náhradní výrobu el. proudu. Zásoby nafty jsou 300 litrů, kdy toto množství bez problémů pokryje několika hodinový výpadek pro celou budovu. Výkon agregátu je dostatečně dimenzovaný na zajištění všech jejích energetických potřeb, tedy nejen ZOS, ale i ředitelství a VZ. Dieselový agregát naskočí neprodleně a zcela automaticky po přerušení dodávky el. proudu z rozvodné sítě, zaměstnanci si toho v podstatě vůbec nevšimnou. Zároveň pracovníkům IT oddělení odchází na jejich služební mobily informativní SMS. Pro případ nutnosti doplnit zásoby nafty zajišťuje pověřený THP zaměstnanec nákup PHM u nedaleké čerpací stanice, popř. lze zajistit přistavení cisterny přímo k agregátu. Při vyhlášení některého mimořádného opatření, zejména krizového stavu, budou případně PHM čerpána z určeného výdejního místa.

Obrázek 2 – Generátor elektrického proudu (zdroj: archív ZZS PK)

4.3.2 Požár budovy

Tato MU naštěstí v historii ani současnosti budovu, v níž je umístěno ZOS, nepotkala. Ostražitost a všechna přijatá opatření v rámci požární ochrany (PO) jsou však na místě, budova ZZS PK v Plzni na Borech je navíc zařazena mezi pracoviště se zvýšeným požárním rizikem díky skladu kyslíku a umístění tlakových kyslíkových lahví v sanitních vozech v garážích. Ložisko požáru může kdykoliv vzniknout technickou závadou, kde je přítomen el. proud, dále pak nelze podcenit ani antropogenní vliv (nedbalost, úmysl).

- **Popis MU**

Požár v budově ZZS PK představuje nebezpečí nejen z důvodů značných finančních škod, ale může dojít k přímému ohrožení zdraví či života zaměstnanců ZZS PK, kteří by se v době požáru v budově nacházeli. Trvalé poškození technologických prvků je vážnou hrozbou s dlouhodobými a finančně nákladnými dopady. Další sekundární hrozbou je i možnost výbuchu v budově, kde je uskladněno mnoho kyslíkových lahví v sanitních vozech stojících v garážích či se tlakové lahve nacházejí přímo ve skladu kyslíku.

- **Příčina MU**

Požár může vypuknout díky technické závadě na některém elektrickém zařízení, nebo nedbalostním jednáním některého ze zaměstnanců. Úmyslné založení požáru přichází v úvahu jako žhářství či jako důsledek teroristického útoku.

- **Následky MU**

Následky požáru v budově záchranné služby v areálu borských kasáren mohou být v podobě snížení počtu výjezdových vozidel a tedy akceschopných výjezdových skupin. Sanitní vozy poškozené či zcela zničené požárem nelze samozřejmě použít při poskytování zdravotních služeb. Vzhledem k tomu, že je výjezdová základna v Plzni na Borech největší v Plzeňském kraji, byly by tyto ztráty citelné. Ve zdravotnickém

úseku by požár poškodil i zázemí záchranářů a sklady zdravotnického materiálu, což by také znamenalo určité ochromení chodu této VZ. Navíc požárem zasažené ZOS, při nemožnosti provizorního chodu po nezbytně nutnou dobu, je třeba okamžitě nahradit záložním pracovištěm, v opačném případě by znamenalo kritické ohrožení jeho funkce a tedy poskytování PNP. Pokud by požár zachvátil i samotný THP úsek, znamenalo by to ochromení veškerého administrativního chodu organizace včetně personálního oddělení, účtáren a archívu. Z výše popsaného tedy vyplývá strategická důležitost a nezastupitelnost této budovy pro „běžný chod“ záchranné služby.

- **Stávající ochranná opatření**

V rámci prevence proti požáru jsou všichni zaměstnanci ZZS PK pravidelně školeni v oblasti PO. Je zakázáno manipulovat s otevřeným ohněm, používat elektrospotřebiče v rozporu s jejich návodem pro použití, zasahovat do el. rozvodů atd. Zároveň je zakázáno v celém objektu kouření – za prvé z důvodu, že záchranná služba je zdravotnické zařízení a za druhé z důvodu, že celý objekt je vybaven elektrickou požární signalizací (EPS). Všichni zaměstnanci jsou proškoleni ze znalostí únikových tras (všechny únikové cesty a únikové východy jsou značeny piktogramy (*obrázek 3 a 4*), rozmístění hasicích přístrojů a hydrantů a vyrozumění při vzniku požáru. Řidiči jsou instruováni, že v případě požárního poplachu musejí vyjet z garáží se všemi sanitními vozy.

Obrázek 3 – Piktogram úniková cesta (zdroj: http://www.eshop-tabulky.cz/-znacky-pro-pozarni-evakuacni-plany/1202-unikova-cesta-vpravo.html)

Důvodem je nejen jejich potřebnost a vysoká hodnota, ale také tlakové kyslíkové lahve, které jsou standardním vybavením všech sanitních vozů. Externí bezpečnostní pracovník provádí namátkové kontroly dodržování zásad PO a ověřuje znalosti zpracované protipožární dokumentace.

Obrázek 4 – Piktogram únikový východ (zdroj: http://www.eshop-tabulky.cz/-znacky-s-textem/3288-unikovy-vychod-text-bez-symbolu.html)

Únikové cesty a únikové východy u budov řeší **vyhláška č. 246/2001 Sb., vyhláška Ministerstva vnitra o stanovení podmínek požární bezpečnosti a výkonu státního požárního dozoru (vyhláška o požární prevenci)**, dále příslušné **České technické normy – ČSN 73 08 34, ČSN 73 08 02** a **ČSN 73 08 04**. Žádná z únikových chodeb v posuzované budově není užší než 2,0 metry. Vzhledem k počtu osob v budově a vzdálenosti k nejbližším evakuačním východům je tak dokonce předimenzována.

DOKUMENTACE POŽÁRNÍ OCHRANY ZZS PK

Nedílnou součástí stávajících ochranných opatření jsou i zpracované dokumenty v rámci PO, jejichž taxativní přehled nám uvádí vyhláška o požární prevenci.

Druhy této dokumentace vycházejí z § 27 dané vyhlášky, kde je uvedeno:

„Odst. (1) Dokumentací požární ochrany se stanovují podmínky požární bezpečnosti provozovaných činností a prokazuje se plnění některých povinností stanovených předpisy o požární ochraně. Dokumentaci požární ochrany tvoří

a) dokumentace o začlenění do kategorie činností se zvýšeným požárním nebezpečím nebo s vysokým požárním nebezpečím,
b) posouzení požárního nebezpečí,
c) stanovení organizace zabezpečení požární ochrany,
d) požární řád,
e) požární poplachové směrnice,
f) požární evakuační plán,
g) dokumentace zdolávání požárů,
h) řád ohlašovny požárů,
i) tematický plán a časový rozvrh školení zaměstnanců a odborné přípravy preventivních požárních hlídek a preventistů požární ochrany,
j) dokumentace o provedeném školení zaměstnanců a odborné přípravě preventivních požárních hlídek a preventistů požární ochrany,
k) požární kniha,
l) dokumentace o činnosti a akceschopnosti jednotky požární ochrany, popřípadě požární hlídky.

Odst. (2) Součástí dokumentace požární ochrany je také další dokumentace obsahující podmínky požární bezpečnosti, zpracovávaná a schvalovaná, popřípadě vedená podle zvláštních předpisů, například požárně bezpečnostní řešení, bezpečnostní dokumentace, bezpečnostní listy, jakož i doklady prokazující dodržování technických podmínek a návodů vztahujících se k požární bezpečnosti výrobků nebo činností, rozhodnutí a stanoviska správních úřadů týkající se požární bezpečnosti při provozovaných činnostech.“

Dokumentace o začlenění do kategorie činností se zvýšeným požární nebezpečím (ZPN) nebo s vysokým požárním nebezpečím (VPN)

K vypracování dokumentace PO a začlenění do kategorií ZPN a VPN musí přistupovat každá podnikající fyzická nebo právnická osoba, musí dále plnit podmínky požární bezpečnosti v ní stanovené a udržovat ji v souladu se skutečným stavem. Dále je

zapotřebí provozované objekty užívat pouze na základě kolaudačního rozhodnutí a požárně bezpečnostního řešení (PBŘ) dané stavby či objektu.

Z projektové dokumentace stavby je patrna nejvyšší možná přítomnost skladovaných nebezpečných látek nebo směsí, kde se budou nacházet nebo skladovat, popř. počtu vyskytovaných osob, únikových východů, evakuačních cest, vybavení prostor věcnými prostředky PO a ostatních věcí, které nám budou sloužit pro doplnění informací při zpracování dokumentace PO.

V následujícím § 28 této vyhlášky o požární prevenci je blíže specifikována **dokumentace o začlenění do kategorie činností se ZPN a s VPN**. Příkladem této dokumentace je „**Prohlášení o začlenění do kategorií podle míry požárního nebezpečí u ZZS Plzeňského kraje“**, které je uvedeno v „příloze A“.

„Dokumentace o začlenění do kategorie činností se zvýšeným požárním nebezpečím a s vysokým požárním nebezpečím (dále jen "začlenění") obsahuje

a) označení druhu provozované činnosti a uvedení místa, kde je tato činnost provozována,
b) uvedení údajů o provozované činnosti rozhodných pro přiřazení charakteristik potřebných pro začlenění,
c) přiřazení charakteristik, kterými jsou definovány činnosti se zvýšeným požárním nebezpečím a s vysokým požárním nebezpečím (§ 4 odst. 2 a 3 zákona) k činnosti a místu podle písmene a),
d) prohlášení právnické osoby nebo podnikající fyzické osoby o začlenění.“
(§ 28 vyhlášky č. 246/2001 Sb.)

„Stanovení organizace zabezpečení PO“ je směrnice, která upravuje vytvoření vlastního organizačního systému, nezbytného pro plnění povinností vyplývajících z předpisů o PO, přitom se vychází z kategorií a rozsahu provozovaných činností. Při zpracování této směrnice musíme postupovat tak, aby dokument obsahoval uvedené náležitosti § 30 vyhlášky o požární prevenci.

„**Požární řády**“ se zpracovávají pro činnosti (pracoviště) se ZPN nebo VPN a zveřejňují se tak, aby byly dobře viditelné a trvale přístupné pro všechny osoby vyskytující se v místě provozované činnosti. Požární řád upravuje základní zásady chování osob na pracovišti. Jeho přílohou musí být spolu s ním vyvěšen jmenný seznam

členů preventivní požární hlídky pracoviště s uvedením jejich úkolů. Při zpracování požárního řádu musíme postupovat tak, aby dokument obsahoval uvedené náležitosti § 31 vyhlášky o požární prevenci. Jako příklad je v „příloze B“ uveden „**Požární řád pro činnost ZPN ve skladu O_2 ZZS Plzeňského kraje“.**

„**Požární poplachové směrnice**“, dále PPS, se zpracovávají pro činnosti (pracoviště) se zvýšeným nebo vysokým požárním nebezpečím a zveřejňují se tak, aby byly dobře viditelné a trvale přístupné pro všechny osoby vyskytující se v místě provozované činnosti. Požární poplachové směrnice vymezují činnosti zaměstnanců, popřípadě dalších osob při vzniku požáru. Při zpracování PPS musíme postupovat tak, aby dokument obsahoval uvedené náležitosti § 32 vyhlášky o požární prevenci. „**Požární poplachovou směrnici ZZS Plzeňského kraje“** máme uvedenu v „příloze C“.

„**Požární evakuační plán**“ se zpracovává pro objekty a prostory, ve kterých jsou složité podmínky pro zásah, nebo kde se provozují činnosti s VPN, a v případě, že tak stanoví dokumentace PO zpracovaná na základě stanovení podmínek požární bezpečnosti, i pro další provozované činnosti se ZPN. Požární evakuační plán upravuje postup při evakuaci osob a materiálu z objektů zasažených nebo ohrožených požárem.

Požární evakuační plán má část grafickou a část textovou. Grafické znázornění směru únikových cest se umísťuje na dobře viditelném a trvale přístupném místě v jednotlivých podlažích objektů a zařízení. Ve stavbách ubytovacích zařízení se grafické znázornění směru únikových cest umísťuje také uvnitř ubytovacích jednotek, zpravidla u vstupu do únikových cest. Při zpracování požárního evakuačního plánu musíme postupovat tak, aby dokument obsahoval uvedené náležitosti §33 vyhlášky o požární prevenci.

„Evakuační plány“ celé budovy ředitelství, VZ Plzeň-Bory i ZOS jsou rozpracovány v kap. 4.3.3 a přílohách F–I.

„**Řád ohlašovny požárů**“ se zpracovává pro činnosti (pracoviště) se ZPN nebo VPN, pokud se jedná o místo s trvalou obsluhou vybavené potřebnými komunikačními prostředky, které je určeno k přijímání hlášení o vzniku požáru nebo jiné mimořádné události.

Řád ohlašovny požárů upravuje způsob přijímání hlášení o vzniku požáru, vyhlášení požárního poplachu pro zaměstnance a další osoby zdržující se na pracovištích právnické osoby nebo podnikající fyzické osoby, oznámení požáru na operační středisko hasičského záchranného sboru kraje a se zřetelem k místním podmínkám. Při zpracování řádu ohlašovny požárů musíme postupovat tak, aby dokument obsahoval uvedené náležitosti § 35 vyhlášky o požární prevenci (pokud je povinnost jej zpracovávat). Příkladem je „**Řád ohlašovny požáru ZZS Plzeňského kraje“** v „příloze D“.

„**Dokumentace týkající se školení**“ – zahrnuje **tematický plán a časový rozvrh školení a odborné přípravy**, dále pak **dokumentaci o provedeném školení**.

Cílem školení je seznámení zaměstnanců s právními a ostatními předpisy, které jsou obsaženy v tématických plánech. Doplňují odborné předpoklady zaměstnanců a požadavky pro výkon daného pracovního zařazení. Pro členy preventivních požárních hlídek a preventistů musí být navíc provedena odborná příprava. Příkladem této dokumentace je **„Zpracování osnov tematických plánů u ZZS Plzeňského kraje“** uvedených v „příloze E“.

Rozsah a způsob školení:

a) U činnosti ZPN provádí školení vedoucích zaměstnanců včetně odborných příprav odborně způsobilá osoba (OZO) nebo technik PO. Školení řadových zaměstnanců provádí proškolený vedoucí zaměstnanec nebo preventista.

b) U činnosti VPN provádí školení vedoucích zaměstnanců OZO nebo technik PO. Odbornou přípravu preventisty a preventivní požární hlídky provádí pouze OZO v oboru PO. Školení řadových zaměstnanců provádí proškolený vedoucí zaměstnanec nebo technik PO.

Výše uvedená dokumentace musí zahrnovat všechny uvedené náležitosti obsažené v § 36 vyhlášky o požární prevenci.

Součástí dokumentace PO jsou dále „**Požární kniha**“, „**Bezpečnostní listy**“ a „**Požárně technické charakteristiky**“, „**Projektová dokumentace**“, „**Požárně bezpečnostní řešení staveb (technické zprávy PO)**“, „**Revizní zprávy na jednotlivá zařízení**“, „**Zápisy z kontrol**“, „**Průvodní dokumentace výrobců zařízení**“, „**Kolaudační**

rozhodnutí resp. dokumentace o povolení užívání stavby“, jiná požárně bezpečnostní dokumentace, např. „**pracovní postupy**“.

Výše uvedená dokumentace musí zahrnovat všechny uvedené náležitosti obsažené v §§ 37–39 vyhlášky o požární prevenci.

4.3.3 Evakuace ZOS z důvodu hrozící MU

Mezi takové MU patří např. ohlášení údajného umístění nástražního výbušného systému v prostorách budovy ředitelství nebo výjezdové základny Plzeň-Bory, popř. přímo v prostorách zdravotnického operačního střediska.

- **Popis MU**

ZOS může být potřeba evakuovat i v jiných situacích, než je jen požár. Krajské město Plzeň bylo během 2. světové války jako průmyslové město s rozsáhlou zbrojní výrobou často bombardováno. Občas se i po letech najde při výkopových pracích nevybuchlá munice. Obzvláště letecké pumy představují značné nebezpečí pro okruh v řádech stovek metrů, kdy musí být při jejich vyzvednutí a následném transportu k likvidaci evakuovány celé ulice či části městských čtvrtí.

Dalším nebezpečím může být nutnost evakuace ZOS pro případ ohlášení údajného umístění nástražního výbušného systému či dokonce nalezení podezřelého nebezpečného předmětu přímo v budově.

- **Příčina MU**

Příčina vzniku takové MU může být buď náhoda, a to v případě zmíněného nálezu nevybuchlé munice z 2. světové války v rámci zemních prací, anebo úmyslný trestní čin v podobě šíření poplašné zprávy či dokonce trestní čin obecného ohrožení.

- **Následky MU**

Pokud nedojde k aktivaci výbušného nástražního systému, tedy k výbuchu s následným devastačním poškozením budovy, resp. přímo pracoviště ZOS s možnými ztrátami na životech, samotná evakuace ZOS, a to z jakýchkoliv důvodů by nepředstavovala výrazné snížení dostupnosti PNP. Před opuštěním pracoviště dochází při minimálním prodlení několika minut k přepojení linek 155 na služební mobily, které jsou k tomuto účelu vyhrazeny. Po opuštění budovy by následoval transport operátorů do prostor záložního operačního střediska, kde by byly zprovozněny všechny potřebné technologie k základním činnostem ZOS.

- **Stávající ochranná opatření**

Vstup do budovy ZZS PK je možný pouze klíči, popř. vstupní kartou přes elektronický systém, nebo vpuštěním do budovy po zazvonění na zvonek kanceláře konkrétního pracovníka. Ten musí zajistit případný doprovod návštěvy po budově. Všechny vstupy do budovy jsou monitorovány kamerovým systémem.

Vstup na ZOS je opět jištěn dveřmi na kartu. Skleněná výplň ve dveřích je navíc kryta speciální fólií, která zabraňuje násilnému vstupu nepovolané osoby na toto pracoviště.

Základním a nezbytným řešením při evakuaci ZOS je však existence záložního pracoviště, s možností jeho využití při mimořádné události, nebo při omezení či výpadku činnosti ZOS v budově ředitelství v Plzni na Borech. Toto náhradní záložní pracoviště musí být nepřetržitě připraveno ke své aktivaci, tedy musí být vybaveno potřebnou výpočetní technikou, spojovacím zařízením a telefonními linkami s připojením na vnější datovou síť nejlépe přes optický kabel.

V současné době je záložní ZOS umístěno v Plzni v Lidické ulici, na výjezdové základně Plzeň-Lochotín, která je vzdálena cca 6 km od mateřského pracoviště. Pokud bude nutné evakuovat zdravotnické operační středisko, je možné volit mezi dvěma scénáři zajištění nepřetržitého provozu tísňové linky 155:

a) Linku 155 přepojí vedoucí směny ZOS na náhradní zmíněné záložní dispečerské pracoviště ZZS PK v prostorách výjezdové základny na Lidické ulici, kam je neprodleně vyslána tříčlenná skupina operátorů – dispečerů. Jejich transport je

zajištěn služebním referentským vozidlem záchranné služby a provádí se vždy s využitím výstražného světelného a zvukového zařízení. Na tomto záložním pracovišti jsou k dispozici počítače s potřebným softwarem. Reálná doba spuštění náhradního dispečerského pracoviště je 10 minut.

b) Tísňová linka 155 bude přepojena na žádost vedoucího směny ZOS na 5 mobilních telefonů, které jsou jen pro tento případ určeny. Nevýhodou tohoto řešení je zhoršení komfortu možnosti si hovor opětovně přehrát, nahrávání telefonátů je přechodně zajištěno jen na vnitřní paměť telefonu. Veškeré řízení činnosti výjezdových skupin se odehrává pomocí zmíněných mobilních telefonů, papíru a propisky bez možnosti přístupu k dalším informačním systémům. Z tohoto důvodu není tato varianta preferována. Reálná doba spuštění náhradního řešení je 5 minut.

V současné době, resp. s výhledem do budoucna, je zvažována nová koncepce záložního ZOS, a to hned na 2 pracovištích HZS Plzeňského kraje. Jedno by se nacházelo v prostorách Krajského operačního a informačního střediska (KOPIS) Hasičského záchranného sboru Plzeňského kraje a druhé pak na požární stanici (PS) HZS Plzeň – Košutka.

První varianta se jeví jako velice výhodná – vzdálenost do 1 km od současného pracoviště, zároveň s možným využitím všech stávajících neporušených systémů ZOS přes optické napojení, rychlý přesun operátorů na záložní pracoviště s minimální časovou prodlevou.

Zásadní a nedílnou součástí evakuačních opatření jsou jejich grafické části, resp. **evakuační plány**. Tyto evakuační plány jsou zpracovány pro jednotlivá podlaží či ucelenější celky, kde jsou graficky znázorněny únikové trasy při vzniku nebezpečí (např. požáru) v daném místě. ZZS Plzeňského kraje má tyto evakuační plány zpracovány pro celou budovu, tedy i včetně ZOS (přílohy F–I)

1. NP je rozděleno dveřmi na tzv. výjezdovou část a THP část. Část výjezdová je určena výjezdovým skupinám, zázemí zde mají řidiči, záchranáři a lékaři. V THP úseku jsou kanceláře útvaru ekonomiky a provozu a také vedení organizace. V tomto sektoru je standardní pracovní doba od pondělí do pátku od 7.00 hod do 15.30 hod. V době pracovního klidu či o státních svátcích je tento trakt zcela prázdný, tedy bez osob.

2. NP se nachází kanceláře IT a technického odd., největší část pak zaujímá zdravotnické operační středisko. ZOS jako režimové pracoviště a zároveň prvek KI je od ostatního provozu odděleno skleněnými bezpečnostními dveřmi, kdy průchod jimi je umožněn jen na čipovou elektronickou kartu.

Poslední přílohou „I“ je v tabulce uspořádaný výčet **únikových tras** s výpočtem jejich kapacity.

4.3.4 Epidemie mezi zaměstnanci

Tato další MU patří také mezi ty, které se sice nepravidelně, ale poměrně frekventovaně vyskytují v běžné populaci, a proto se nemusí nevyhnout ani zaměstnancům ZZS PK, resp., přímo ZOS.

- **Popis MU**

Epidemií mezi zaměstnanci se rozumí rozšíření infekční choroby mezi zaměstnanci, kdy dojde k velkému nepoměru mezi práce schopnými a neschopnými.

- **Příčina MU**

Mezi nejpravděpodobnější patří rozšíření některého virového onemocnění v pracovním kolektivu, a to kapénkovým způsobem. Učebnicovým příkladem může být chřipka. Nakazit se chřipkovým onemocněním je obzvláště v době epidemie pro členy výjezdových skupin velice jednoduché, protože se během služby nacházejí v úzkém kontaktu s nemocnými, kterým poskytují péči. Ti se pak, sice omezeně, ale přeci jen dostávají i do styku se zaměstnanci ZOS.

Hrozbu představují i epidemie vyvolané závadným jídlem, tedy alimentární otravy. V tomto případě je hrozba v podobě salmonelózy při sezónním výskytu během letních měsíců. Rozvážková forma závodního stravování, a tudíž větší počet konzumentů stejného pokrmu při nedodržení všech hygienických předpisů, nahrávají možnému vzniku této MU s následnou velkou pracovní neschopností.

- **Následky MU**

V případě vypuknutí epidemie mezi zaměstnanci nedojde k narušení poskytování PNP v Plzeňském kraji, může však nastat přechodná personální nouze, která je jen díky přijatým předem připraveným opatřením eliminována.

- **Stávající opatření**

Naše organizace hrozbám v podobě možného hromadného onemocnění operátorů či záchranářů čelí vzájemnou zastupitelností zaměstnanců. Část dispečerů ZOS slouží jako záchranáři ve výjezdových skupinách a naopak část záchranářů má částečný úvazek na ZOS. Tímto je docíleno možnosti v případě potřeby nahradit nemocné zaměstnance jinými. Samostatnou kapitolou jsou lékaři. Jejich nedostatek by byl řešen jejich zastoupením lékaři z jiných oblastí.

Pro poskytování PNP pacientovi s podezřením na vysoce nakažlivou nemoc (VNN) je předurčen od roku 2011 ***tzv. Bio Hazard Team (BHT)***, který je vybaven speciálními osobními ochrannými pracovními pomůckami (OOPP), a hlavně pravidelně nacvičuje tento zásah za použití biovaku. Plzeňský BHT byl již několikrát na specializovaném výcviku v nejmodernějším zařízení v ČR, a to v Centru biologické ochrany (CBO) Těchonín (*obrázek 5*). CBO je armádní objekt charakteru nemocnice, pracující v přísném protiinfekčním podtlakovém režimu s nejvyšším 4. stupněm biologické bezpečnosti (ochrany), tzv. BSL4 (**B**io**S**afety **L**evel).

Velký důraz je samozřejmě kladen na prevenci vůči jakýmkoli infekčním chorobám. Zásadním se jeví správné a časné používání OOPP (např. ochranných roušek, resp. masek, ochrana spojivek, apod.) a striktní dodržování bazálních hygienických návyků i předpisů.

Obrázek 5 – Bio Hazard Team na výcviku v CBO Těchonín (zdroj: archív ZZS PK)

Každý sanitní vůz ZZS PK je vybaven tzv. protiinfekčním balíčkem který obsahuje: kombinézy Microguard 2500, návleky na obuv, ochranné roušky FFP3, jednorázové zástěry, ochranné brýle, lepicí pásku.

4.4 Nejpravděpodobnější rizika v rámci novodobých hrozeb

Jak již bylo pojednáno v teoretické části, mezi novodobá rizika či novodobé hrozby řadíme ***tzv. kybernetickou bezpečnost***. K provedení analýzy stávajícího stavu na ZOS v rovině této problematiky je nejprve nutné popsat celou infrastrukturu, včetně softwaru (SW) a hardwaru (HW), ICT techniky a také popsat vzájemné vazby těchto prvků, tok elektronických dat včetně jejich ochrany, uchovávání a zálohování.

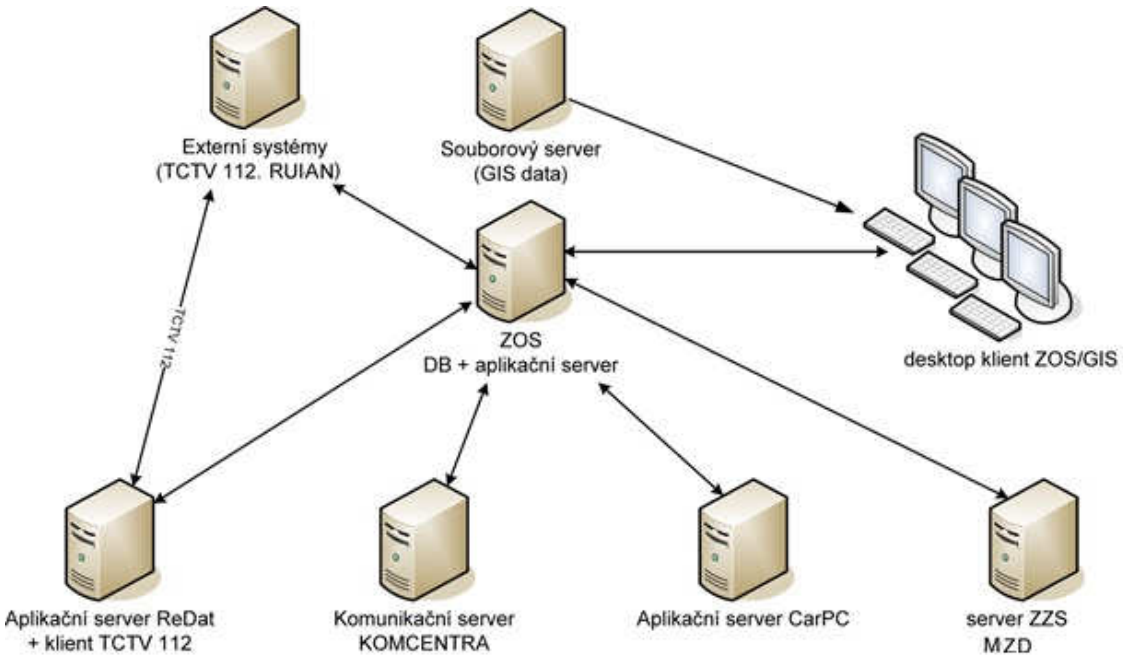
4.4.1 Popis infrastruktury ZOS

Zdravotnické operační středisko od dob, kdy vznikla záchranná služba v plzeňském regionu v roce 1974, opravdu prošlo svým vývojem od pomyslné doby kamenné, přes průmyslovou až po vědecko-technickou revoluci dnešních dnů. Začátky, kdy postačovala tužka a papír, mapa v papírové podobě a telefon s kulatým vytáčejícím ciferníkem, jsou nenávratně pryč. Dnešní ZOS je plně modernizovaným pracovištěm s technologiemi 21. století, které jsou velice sofistikované a vyžadují kvalifikovaný personál, který je umí ovládat. „Slabinou“ takového provozu je právě jeho technologická složitost a jeho přímá závislost na elektrické energii, kdy při výpadku některého prvku – segmentu či energetického zdroje může nastat určité omezení chodu pracoviště a tak ohrožení jeho primární funkce. V následující kapitole se budeme zabývat vybavením ICT a také kybernetickou bezpečností tohoto pracoviště.

- **Fyzická architektura subsystému ZOS**

Na uvedeném schematickém *obrázku 6* je znázorněna fyzická architektura ZOS. Tato fyzická architektura systému ZOS se skládá z několika částí, mezi kterými jsou znázorněny i jejich vazby:

- **server systému ZOS** (hlavní server) slouží současně jako databázový server a aplikační server;
- **komunikační server** pro rádiovou komunikaci s výjezdovými skupinami (VS)



Obrázek 6 – Znázornění fyzické architektury serverového systému ZOS
(zdroj: PER4MANCE s.r.o. – systémová dokumentace)

a jinými subjekty je osazen řešením od firmy KOMCENTRA, přes který se ovládají i hlasová pojítka přímo ze ZOS;

- **aplikační server záznamového systému ReDat** odesílá do IS ZOS data hovorů
- **interní aplikační servery** ZZS PK slouží pro komunikaci s VS – server pro distribuci zpráv CarPC; komunikace s aplikačními servery ZZS PK je nutná pro zajištění integrace IS ZOS se **systémem CarPC (Fleetware Radium);**
- **aplikační server systému MZD** (mobilní zadávání dat) přijímá z dispečerského systému data o výjezdu a pacientech přímo do tabletu posádky; ten pak slouží pro vytváření dat v rámci výjezdu a vedení EKP (elektronické karty pacienta);
- **externí aplikační servery**, se kterými server ZOS komunikuje, jsou aplikační **servery tísňové linky 112 TCTV/NIS IZS**, **server pro aktualizace registru RÚIAN**, apod.

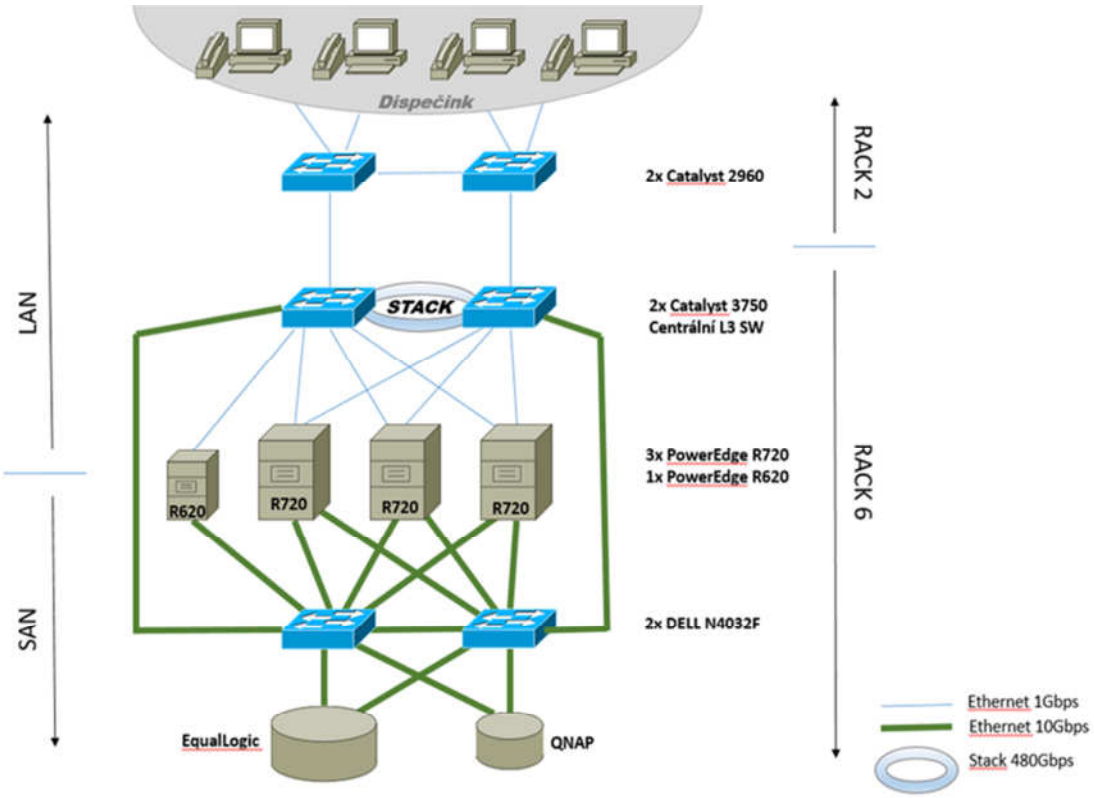
4.4.2 Hardware

Hardwarové vybavení můžeme rozdělit do 3 velkých skupin, a to **serverové vybavení, koncová zařízení s terminály** a **zařízení zajišťující energetickou stabilitu**.

Prostředníkem mezi klientem, resp. koncovými zařízeními (terminály) a vlastním hardwarem PC (serverem) je interface s názvem „**proxy server**“ (*proxy angl. znamená v zastoupení, prostřednictvím zástupce*). Může se jednat jak o specializovaný HW, tak o SW. Proxy server odděluje např. lokální počítačovou síť (LAN) jako např. **INTRANET** od rozsáhlé sítě (WAN), tedy např. **INTERNETU**.

- **Servery**

Základem serverové infrastruktury na *obrázku 7* jsou virtualizační servery firmy DELL PowerEdge R720 vybavené připojení 10 Gbps a doplněny pro pokročilou vzdálenou

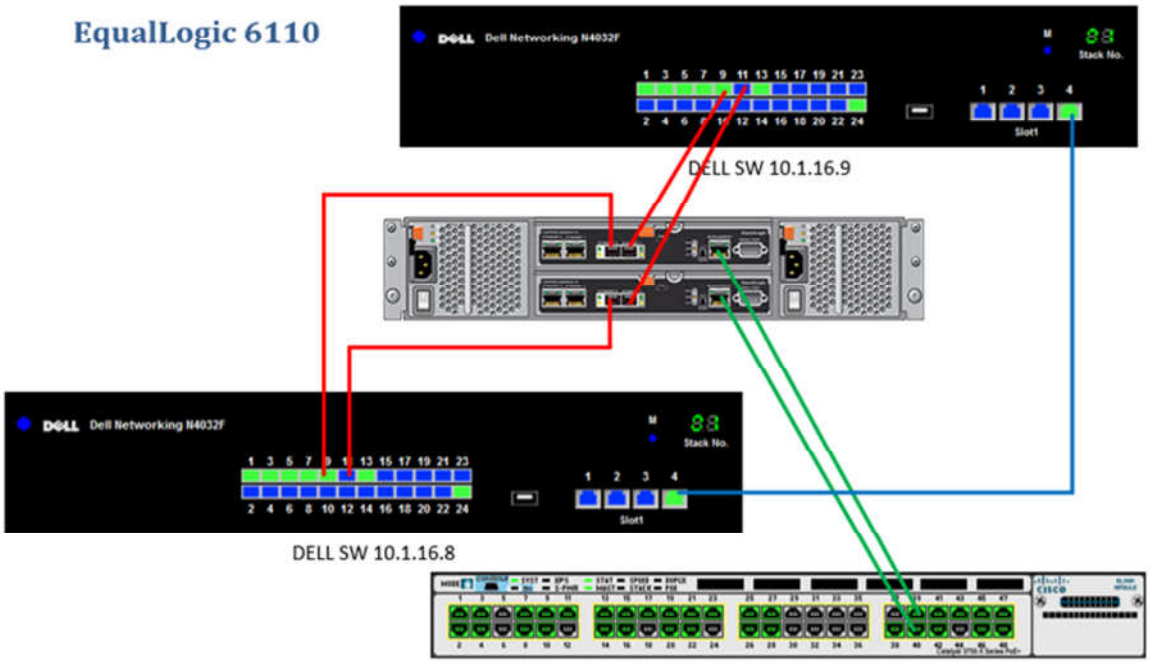


Obrázek 7 – HW serverová infratruktura ZOS

(zdroj: PER4MANCE s.r.o. – systémová dokumentace)

správu o technologií **Integrated Dell Remote Access Controller 7 (iDRAC7)**. Servery tvoří virtualizační platformu pro provoz všech serverů (jeden server je vyhrazen pro dispečerský SW SOS). Tyto servery jsou doplněny o server pro centralizované řízení DELL řady **PowerEdge R620**, který je také vybaven rozhraním 10 Gbps a iDRAC7.

Pro diskové operace je infrastruktura vybavena **datovým úložištěm DELL EqualLogic řady PS6110 10 Gbps iSCSI** s redundantními řadiči (*obrázek 8).* Toto diskové pole slouží pro provoz všech virtuálních serverů v rámci operačního řízení.
Úložiště je doplněno dvěma **switchi DELL v konfiguraci s 24 porty 10 Gigabit Ethernet** pro vytvoření oddělené SAN network, které umožní i budoucí rozšíření o další disková pole a servery. SAN na bázi iSCSI je tedy provozováno na oddělené 10 Gbps sítě.
Do infrastruktury je připojeno i **zálohovací úložiště QNAP NAS s 10 Gbit rozhraním**, na který jsou pravidelně zálohovány jednotlivé servery, a umožňuje i zprovoznění těchto serverů z tohoto úložiště. (PER4MANCE s.r.o., 2017)



Obrázek 8 – Datové úložiště DELL EqualLogic řady PS6110 10 Gbps iSCSI s redundantními řadiči (zdroj: PER4MANCE s.r.o. – systémová dokumentace)

- **Klientské terminály a koncová zařízení**

Všechna dispečerská pracoviště na ZOS jsou vybavena výškově nastavitelnými stoly odpovídající požadavkům na umístění operátorského pracoviště a osazena následujícími technologiemi:

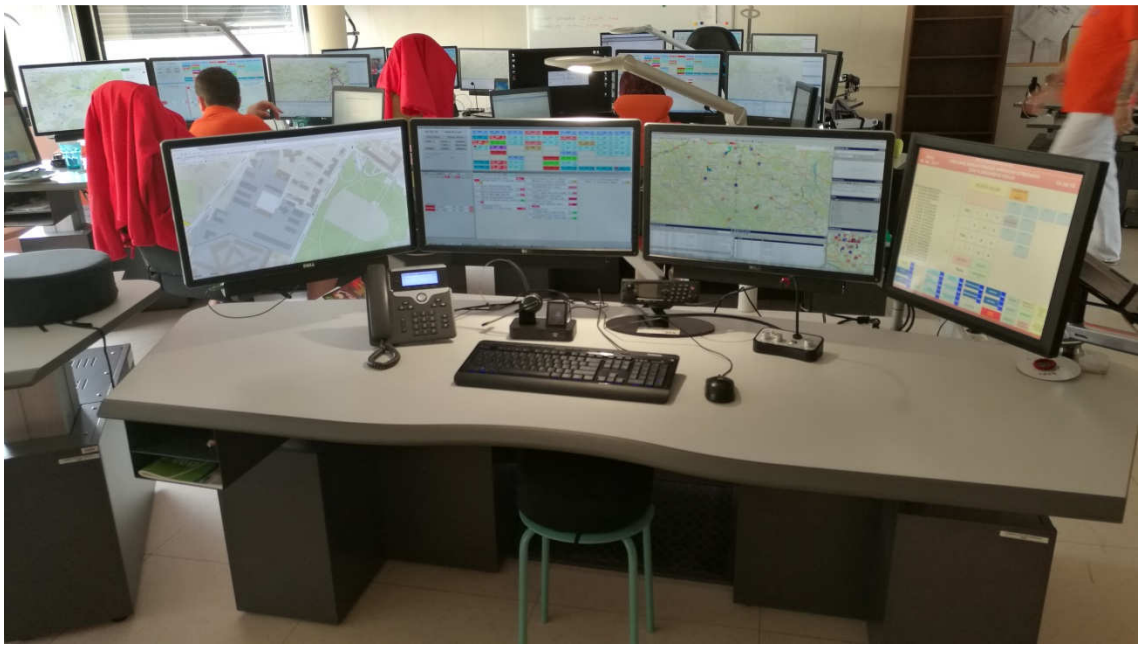
- pracovními terminály;
- monitory – 3 x LCD a 1 x dotykový monitor na jedno pracoviště;
- technologií na distribuci audia (přepínání audia vstupů), náhlavní HandsFree setem, integrací telefonie a rádiového provozu (digitálního i analogového);
- komunikační integrací na řízení hovorů.

Pracovní terminál umožňuje připojení prostřednictvím protokolů PCoIP k **centrálnímu virtualizačnímu prostředí (VMWare View)** a provozovat tak virtuální desktop pracoviště. Jako pracovní terminál je použit **terminál HP s Windows® Embedded Standard 7**. (PER4MANCE s.r.o., 2017)

Terminál připojuje všechny dispečerské monitory včetně dotykového monitoru pro ovládání hlasové komunikace. Celá infrastruktura dispečerského pracoviště je koncipována tak, aby bylo možné dispečerské pracoviště provozovat jak prostřednictvím stávajícího terminálu, tak případně samostatným PC.

Dispečerské pracoviště (*obrázek 9*) je tak vybaveno jedinou klávesnicí a myší připojené do terminálu. Dispečer má k dispozici celkem 3 monitory (operační řízení SOS, GIS, ostatní aplikace) a jeden dotykový monitor pro ovládání hlasové (telefonní/radiové) komunikace. Pro provoz hlasové komunikace je dispečer dále vybaven **bezdrátovou náhlavní soupravou JABRA**.

Pro záložní řešení Telefonie je na každém dispečerském stole umístěn fyzicky IP Telefon a v rámci dispečinku jsou i umístěny samostatné radiostanice.



Obrázek 9 – Dispečerské pracoviště na ZOS (zdroj: vlastní foto)

- **Zálohování napájení**

Nedílnou a velice potřebnou částí HW vybavení jsou záložní energetické systémy buď ve formě záložních baterií neboli **UPS** (z angl. **U**ninterruptible **P**ower **S**upply/**S**ource, zdroj nepřerušovaného napájení), tedy zařízení, které zajišťuje souvislou dodávku elektrické energie pro spotřebiče, které nesmějí být neočekávaně vypnuty. Komplexním řešením pro větší celek je pak zařízení, které znamená již určitou energetickou soběstačnost, např. pořízením **diesel agregátu** (viz také kap. 4.1.1).

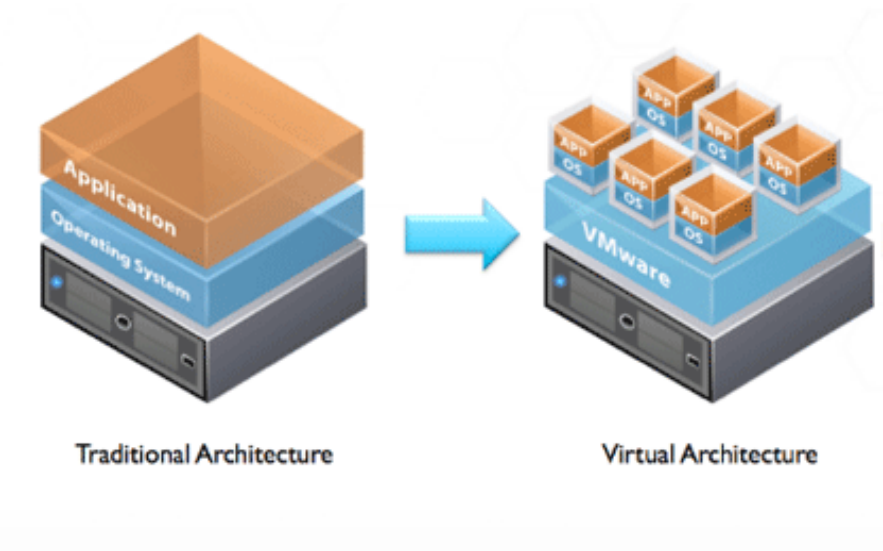
4.4.3 Software

Základním prostředkem pro efektivní využití HW i SW je v dnešní době virtualizace. Její rozvoj umožnila **tzv. VM technologie** (Virtual Machine, virtuální stroj), kdy na obchodním poli s touto komoditou se pohybuje několik důležitých hráčů jako IMB, Apple Inc., VMware, Inc. a další.

- **Virtualizace**

Podstatou virtualizace je provoz více oddělených serverů na jednom fyzickém hardware. To přináší zásadní úspory v pořizovacích i provozních nákladech, zlepšuje správu, urychluje vytvoření a nasazení nového serveru a další výhody. (WEDOS Internet, a.s., 2017)

Plná virtualizace umožňuje souběžný běh několika virtuálních strojů (s neupravenými operačními systémy) vedle sebe paralelně na jednom fyzickém serveru. Hardware neboli zdroje jsou pro tyto virtuální servery simulovány hypervizorem. Zároveň tyto operační systémy běží od sebe izolovaně, takže se navzájem nijak neovlivňují. Pro lepší představu je na *obrázku 10* vlevo klasická architektura (jeden fyzický server, jeden



Obrázek 10 – Schéma klasického serveru a serveru s virtualizační vrstvou (zdroj: PER4MANCE s.r.o. – systémová dokumentace)

operační systém /OS/) a vpravo jeden fyzický server s virtualizační vrstvou a na něm několik virtuálních serverů, každý s vlastním OS. (RUEST, 2010; ŠIKA, 2012; PER4MANCE, 2017)

Pro správu virtualizovaného prostředí slouží **tzv. vSphere klient**.

- **Jednotné SW vybavení dispečerského pracoviště na ZOS**

Každé dispečerské pracoviště neboli klientský terminál je vybaven následujícím SW **(SOS, GIS, Komcentra, Telefonie, Paeging)**, jehož funkce využívá dispečer – operátor ZOS k vlastní činnosti, tedy k operačnímu řízení.

- **Dispečerský systém SOS**

Základním systémem operačního řízení je **dispečerský systém SOS.** Systém je provozován na databázovém systému ORACLE s jasně definovanými oprávněními a logováním aktivit, tak aby bylo možné dohledat takřka všechny změny dat. (BRYLA a LONEY, 2009)

- **GIS – napojení na sledování vozů**

Subsystém sledování vozů je podpůrným systémem umožňujícím získávání polohy jednotlivých prostředků a jejich stavu pro řízení operační situace. Název SW vychází z jeho primární funkce, tedy jedná se o geografický informační systém (z angl. **G**eographic **I**nformation **S**ystem). Nejedná se tedy o kritická data operačního řízení (OŘ), ale o podpůrný systém, umožňující efektivnější řešení jednotlivých činností ZZS.

- **Hlasová komunikace**

Hlasová komunikace je realizována jak vlastní telefonní komunikací, tak radiovou komunikací.

Telefonní komunikace probíhá na bázi **technologie IP Telefonie** a je z hlediska datového přenosu oddělena do úplně samostatné VLAN (virtuální lokální síť). IP Telefonie pro operační řízení je již realizována vyhrazeným ISDN (digitální síť

integrovaných služeb) připojení pro linku 155. Tato linka je zálohována GSM telefony pro případ výpadku.

Radiová komunikace v rámci radiové sítě PEGAS je realizována také v oddělené VLAN, která je realizována až do lokality krajského ředitelství policie (KŘP) na LCT radiové moduly umístěné na KŘP a ovládaná CC-API serverem dodavatele sítě PEGAS. Vlastní komunikace a celá síť je zabezpečená a provozována MV ČR pro všechny složky IZS.

Integrujícím prvkem je **tzv. integrace hlasového provozu** realizovaná na aplikacích a technologiích firmy KOMCENTRA. Jedná se v podstatě o společné ovládání hlasové komunikace (telefonní/radiové). Vlastní řešení zabezpečení komunikace je realizováno proprietárním způsobem (šifrou).

- **Paging**

Pagingový systém slouží v rámci ZZS PK jako záložní systém pro informování členů výjezdových skupin ZZS o aktivaci této VS na primární či sekundární zásah. Každý člen VS je vybaven přijímačem (**pagerem**), který buď vydává určitý zvukový signál či je dokonce schopen přijímat a zobrazovat krátké textové zprávy, pokud je zároveň vybaven malým displejem. K přenosu signálu či těchto krátkých zpráv se využívá samostatné radiové sítě. V rámci pagingu lze oslovit více příjemců v jeden okamžik a optimalizovat tak přenos informací.

V rámci dispečerského systému SOS je systém pagingu plně integrován a při potřebě oslovit konkrétní výjezdovou skupinu funguje naprosto autonomně.

- **MZD - Mobilní zadávání dat / EKP – Elektronická karta pacienta**

Se SW MZD dispečerské pracoviště přímo nepracuje, tento SW je nahrán na tabletech VS a dispečerský systém pouze posílá data do MZD a ten už si je zpracovává sám podle vlastního algoritmu.

Jelikož MZD je mobilní aplikace provozovaná výjezdovými skupinami ZZS v terénu, pro komunikaci s dispečinkem je pro přenos dat využívána síť GSM. EKP je SW aplikace nainstalovaná na VZ na jednotlivých PC, která slouží pro doplnění chybějících dat o pacientovi či samotném výjezdu. Operátoři ZOS sice nemají přímý přístup

do těchto aplikací, ale některá data jsou automaticky oboustranně aktualizována mezi těmito servery, tedy mezi SOS a MZD/EKP.

4.4.4 Síťová infrastruktura

Výpočetní technika ve 20. století naznala velkého boomu jak na poli HW, tak SW. Významným milníkem se stala nejen virtualizace (viz předchozí kap.), ale ještě dřívější vzájemné propojování HW, tedy jednotlivých PC do lokálních sítí, následně propojování PC na velké vzdálenosti až po samotné vytvoření nadnárodních sítí, mezi které patří v dnešní době právě **INTERNET**.

- **Historie informačních sítí**

Historie se začala psát v roce 1962, kdy v instituci Advanced Research Project Agency v USA byl započat vojenský projekt, který dostal název **ARPANET** a byl prvním předchůdcem internetu. Tato síť byla spuštěna v roce 1969. V roce 1985 americká nadace National Science Foundation začíná budovat vysokorychlostní síť **NSFNET**, určenou pro akademickou sféru. Na počátku devadesátých let 20. století převzal NSFNET roli ARPANETu jako páteřní sítě internetu a otevřel se i pro komerční užití. V roce 1991, kdy odstartovala služba **World Wide Web** (zkráceně web nebo WWW), tedy systém vzájemně propojených tzv. hypertextových dokumentů umístěných kdekoliv v síti internet, což znamenalo další posun v rozvoji této sítě. (KUROSE, ROSS 2014)

U nás se začala historie INTERNETu psát v tehdejší České a Slovenské federativní republice (ČSFR) na počátku 90. let minulého století. První pokusy o připojení do Internetu proběhly v listopadových dnech roku 1991, kdy datová linka vedla z Prahy (ČVUT) do internetového uzlu v Linci. Zprvu šlo pouze o komutovaný spoj („volání do uzlu“), jenž byl později nahrazen pevnou linkou. **Dne 13. února 1992** probíhá slavnostní oficiální připojení naší republiky k Internetu, a to právě na pražském ČVUT. Byla nám přidělena vrcholová doména (přípona za názvem adresy) „**.cs**“. Tato doména měla ale jepičí život, jelikož 1. ledna 2003 dochází k rozdělení tehdejší ČSFR na 2 suverénní státní útvary – Českou republiku a Slovenskou republiku, kterým byly přiděleny současné vrcholové domény „**.cz**“ a „**.sk**“.

- **Infrastruktura ZOS a ZZS PK**

Infrastruktura ZZS je koncipována jako **jedna centrální síť**, ve které je umístěn i dispečink operačního řízení ZZS a výjezdové základny napojené přes **WAN síť** (rozsáhlá síť). ZOS má kromě vlastní WAN sítě ZZS dále napojení na externí sítě, a to do **sítě Internet**, **sítě ITS MV** a **sítě PEGAS** krajského střediska PČR, tedy integrovaného operačního střediska Krajského ředitelství policie Plzeňského kraje (IOS KŘP PK):

- WAN síť ZZS;
- síť Internet;
- síť ITS MV;
- síť PEGAS.

Pozn.: **ITS MV ČR (integrovaná telekomunikační síť Ministerstva vnitra ČR)** – jedná se o technické prostředky a organizační opatření sloužící k propojení objektů jednotlivých subjektů – MV ČR, PČR, IZS a územních orgánů státní správy. Jedná se o privátní síť, která je budována a provozována pro zabezpečení požadovaných telekomunikačních služeb – radio a telefonického spojení a datového spojení.

A. Vnitřní infrastruktura

Základem komunikační infrastruktury jsou centrální L3 přepínače (switche), které vytváří jednotlivé VLAN v lokalitě. Jedná se o **switche Cisco 3750** zapojené do **tzv. stacku**, který vytváří virtuální switch z více fyzických switchů (str. 45, obrázek 7). Tato technologie umožňuje redundanci („přetékání“) a při výpadku jednoho ze switchů je ovlivněna pouze skupina zařízení fyzicky připojená do tohoto switche. Všechny ostatní centrální funkce typu routrování VLAN, omezení provozu apod. přechází na další ze switchů daného stacku.

V současné době jsou servery operačního řízení a dispečerské pracovní stanice z hlediska počítačové sítě umístěny v samostatné VLAN. Proto i napojení ostatních technologií je v maximální míře řešeno redundantně (do dvou switchů centrálního stacku).

Pro oddělení interní sítě ZZS od veřejných a partnerských sítí slouží **centrální FireWall Cisco ASA**, který definuje jednotlivé publikace a oprávnění v rámci připojení těchto sítí. FireWall odděluje nejen síť Internet, která je důležitá pro provoz ZZS a např. intergraci MZD, ale i napojení na Národní informační systém integrovaného záchranného systému (NIS IZS 112) pro kooperaci složek IZS a také sítí krajských zdravotnických zařízení.
Dále je v centrální lokalitě umístěno i připojení do WAN sítě ZZS PK, které zajišťuje připojení všech lokalit ZZS do jedné transparentní WAN sítě.
Veškerá centrální infrastruktura je umístěna v servrovně. Vlastní kabeláž propojení jednotlivých rozvaděčů je realizována v dvojité podlaze serverovny. Pro kabeláž v rámci celé budovy je použit **standard UTP kabeláže kat. 5E**. Kabeláž je rovněž ukončena v servrovně, kde jsou jednotlivé komponenty propojeny do odpovídajících technologií.

B. Vnější infrastruktura

Veškeré lokality ZZS PK jsou propojeny prostřednictvím **zabezpečeného připojení (IPSec, VLAN)** do WAN sítě ZZS. Pro vytváření takové sítě jsou využity technologie:

- Internet připojení a šifrování na bázi IPSec (3DES/AES), připojení výjezdových základen je buď „*optikou*“ *(metropolitní síť CamelNet,* kterou spravuje Plzeňský kraj, připojeno 6 VZ), anebo *ADSL – nakonfigurované VPN* (provozovatelem je O2 Czech Republic a.s.).
- Vyhrazené optické spoje (např. napojení na HZS, PČR apod.)

Základ WAN sítě pro ZZS spravuje právě externí subjekt O2 Czech Republic a.s., který zajišťuje konfiguraci a zabezpečení interní sítě ZZS.

4.4.5 Zabezpečení

Základním bezpečnostním prvkem každého PC, zejména při jeho připojení na externí sítě jako je internet, je příslušný **antivirový program** (např. ESET NOD 32 Antivirus, AVG, Kaspersky Antivirus, AVAST, Norton AntiVirus, Microsoft Defender a další).

Jedná se o počítačový software, který slouží k identifikaci, odstraňování a eliminaci **počítačových virů** (např. rezidentní a nerezidentní viry, stealth viry, makroviry a další) a jiného škodlivého softwaru, souhrnně jde o **tzv. malware** (např. Trojani – trojské koně, worm – červi, crimeware, spyawre, adware, apod.). K zajištění této úlohy se používají dvě odlišné techniky:

- Prohlížení souborů na lokálním disku, které má za cíl nalézt sekvenci strojového kódu odpovídající definici některého počítačového viru v databázi.
- Detekce podezřelé aktivity nějakého počítačového programu, který může značit „infekci“. Tato technika zahrnuje analýzu zachytávaných dat, sledování aktivit na jednotlivých portech či jiné techniky.

Dalším nezbytným bezpečnostním prvkem je **tzv. FireWall**. V počítačové terminologii se firewallem nazývá software (**software firewally**) či hardware (**hardwareové firewally**), jehož funkcí je kontrolovat (povolovat či zakazovat) komunikaci v počítačové síti na základě daných pravidel. Používá se na oddělování různých částí sítě (nejčastěji odděluje nebezpečný internet od místní sítě). V dnešní době je i standardem pro operační systémy Windows. (STREBE a PERKINS, 2003)

Software firewall je buď integrovaný v operačním systému, nebo jej můžeme instalovat jako samostatný software, popř. i takové, které jsou integrovány přímo do antivirových programů, jako například NOD32 (používáno na ZZS PK). Softwarový firewall není tak účinný jako hardwarový.

A. Zabezpečení infrastruktury

Vlastní operační středisko má napojení na vlastní WAN síť ZZS a napojení do externí sítě Internet, sítě ITS MV a sítě PEGAS krajského střediska PČR ČR.

Systém operačního řízení na jednotlivých dispečerských terminálech se skládá jak ze serverů poskytujících potřebné systémy pro samotný chod, tak pro podporu této činnosti hlasovými komunikačními prostředky (telefonie, radioprovoz).

V současné době jsou **servery operačního řízení** a **dispečerské pracovní stanice** z hlediska počítačové sítě umístěny v samostatné VLAN. Tyto VLAN lze následně oddělit i bezpečnostním prvkem (**FireWall**) vyhrazeným pro oddělení interní sítě ZZS

a sítě operačního řízení. Tato část na ZZS není nyní realizována, ale lze ji kdykoliv doplnit, případně řešit jednoduchými access listy na centrálním L3 prvku (viz kap. 6).

Přístup k jednotlivým serverům je řešen prostřednictvím autentizace a autorizace v rámci **Active Directory (AD) Microsoft Windows domény**. Vlastní nastavení jak síly hesla, tak platnosti hesla podléhá centrálním politikám nastaveným v rámci AD Windows domény.

Autentizace a autorizace v rámci AD Windows domény je využívána také pro vzdálený přístup do sítě ZZS ze sítě Internet. Pro VPN připojení se využívá přístupu přes centrální FireWall. Vlastní VPN připojení je realizováno **Cisco VPN klientem** se šifrováním 3DES, AES a SSL. Je tak zaručeno maximální zabezpečení a šifrování přenášených dat v rámci VPN připojení. Všechny vzdálené VPN přístupy jsou logovány v rámci **autentizačních serverů RADIUS (IAS/NPS Windows služba)**.

Pro zabezpečení přístupu **do externích sítí Internet** a **ITS MV ČR** je využíván přístup přes **centrální FireWall**, který provádí omezení komunikace jak z externích sítí, tak i směrem do nich. Přičemž jak do sítě Internet, tak do sítě ITS jsou prostřednictvím centrálního FireWallu publikovány jednotlivé servery/služby. Stávající FireWall podporuje v současné době podporované a doporučované šifrovací protokoly. Log centrálního FireWallu je logován na monitorovací server pro případný audit provozu z/do externích sítí.

Propojení **do radiové sítě PEGAS** je realizováno samostatným datovým okruhem a je opět odděleno v samostatné VLAN pro radiovou síť. Připojení na PČR je realizováno bez průchodu centrálním FireWallem a je koncipováno jako propojení pouze pro hlasovou komunikaci v zabezpečené síti PEGAS, kterou spravuje MV ČR. **Digitální hovorová data radiové sítě PEGAS** jsou během přenosu šifrována jak v síti ZZS,
tak v síti PEGAS. Telefonní komunikace je až do místa pracoviště, včetně telefonního přístroje, zabezpečena na úrovni samostatné oddělené VLAN a vyhrazené ISDN přípojky pro linku 155. Celá integrace je koncipována tak, aby byla využitelné pouze z dispečerských stanic, speciálně nakonfigurovaných.

Na **připojení do sítě ITS** je realizována publikace **samostatného serveru SOS5** pro příjem datových vět národního systému NIS IZS. Tento server je oddělen

od produkční databáze OŘ a do této databáze přenáší až formalizovaná data. Naproti tomu ze sítě ITS jsou získávána data jednotlivými systémy/podsystémy jako jsou GIS systémy, sledování vozů apod. Přístup do sítě ITS je realizován prostřednictvím sítě internet pomocí **technologie PAT (port adress translation)** a nevyžaduje tak přístup na jakoukoliv jinou službu interních serverů operačního řízení. (PER4MANCE s.r.o., 2017)

B. Zabezpečení přístupu z vnějších sítí

Komunikace uživatelů připojovaných zvenčí (WAN) je dostatečně zabezpečena standardními prostředky zabezpečujícími VPN připojení.

- ***Webové služby (WS) pro zpřístupnění dat z/do SOS***

WS řeší pro externí subjekty (mimo běžně přihlášené uživatele SOS) dostupnost pouze nadefinovaných dat a služeb rozhraní webové služby v předem omezeném rozsahu. WS umožňuje předávat/přijímat do/od vnějšího subjektu **autentizovaného vlastním accountem a heslem** příslušné data v přesně omezeném rozsahu bez možnosti přímého přístupu k databázi SOS

Pro poskytování dat na WS je vybudována **aplikační mezivrstva pro oddělení aplikační logiky** koncové externí aplikace spolupracující se SOS a databázového dotazu vzniklého k realizaci požadavku WS přímo do databáze. V aplikačním rozhraní WS je definováno pro použití jen pro omezené množství databázových dotazů a objektů a funkce rozhraní WS tyto dotazy následně sekundárně transformuje do dotazů do DB s omezenými oprávněními pouze pro potřeby předání výsledků/odezvy pouze pro danou funkci – WS je omezena pouze na předem naprogramované činnosti a není technicky možné dostat se k jiným datům než těm, které jsou zpřístupněna pro příslušné aplikační rozhraní WS.

- **Zabezpečené interface pro přebírání dat z jiných subsystémů**

Pro příjem dat z externích subsystémů se využívají **dedikované databázové tabulky** jako interface pro zasílání zpráv do SOS. Ty jsou dostupné externím uživatelům – aplikacím pomocí databázových grantů omezených jen na tyto interfacové tabulky a externí subsystém z databáze nevyzíská žádné další informace. Samotné zpracování

dat z interface dále do SOS probíhá pomocí další samostatných vnitřních procesů SOS s přenosem přijatých informací do dalších aplikačních oblastí SOS Venkovní uživatel tak díku omezením nedokáže z databáze vyzískat žádné další informace, ani narušit integritu dat v jiných databázových objektech.

Využívaným externím subsystémem pro operační řízení jsou např. **mobilní aplikace MZD** provozované výjezdovými skupinami ZZS v terénu, kdy přenos dat mezi ZOS a VS je zprostředkován pomocí GSM sítě operátora. Pro tyto účely je publikován aplikační server MZD do sítě Internet. Tuto komunikaci je možné řešit po dohodě s GSM operátorem také v rámci **privátního APN** (jméno přístupového bodu na internet), kde je zajištěno oddělení datových přenosů od běžného internet provozu. Přihlášením mobilního přístroje k APN poskytovatele se aktivuje mobilní přístup k internetu, aplikační server je oddělen od vlastního databázového serveru.

Obdobně jsou získávána **data o poloze vozidel (GIS)**, kdy opět prostřednictvím sítě GSM jsou zasílána data jak o poloze a provozu jednotlivých prostředků, tak i informace o změně statusu prostředku (fáze výjezdu dané výjezdové skupiny). Subsystém sledování vozů nepracuje s kritickými daty pro operační řízení, ale jedná se o podpůrný systém umožňující efektivnější řešení jednotlivých činností ZZS.

Internetové připojení je dále využíváno systémy/podsystémy operačního řízení k získávání a odesílání dat, např. se jedná o získávání **dopravních informací z Národního dopravního informačního centra (NDIC)** do **systému GIS** odesíláním informací o dopravních nehodách a uzavírkách. Provoz je realizován přes centrální FireWall bez nutnosti publikace serverů.

C. Ochrana IS OŘ ZOS – SOS

Základním a nejdůležitějším systémem operačního řízení je **dispečerský systém SOS.** Systém pracuje na databázi ORACLE, která umožnuje cíleně dohledat takřka všechny změny dat. Jsou zde jasně definovaná přístupová oprávněními a logování těchto aktivit.

- **Bezpečnost z pohledu uživatele (operátora)**

  a) Uživatelská práva a ověřování

Přistup do této databáze je technicky umožněn jen oprávněným uživatelům autentizovaných pod **accountem** (jednoznačným uživatelským jménem) a **heslem**. Každý uživatel SOS má své heslo a je jednoznačně identifikován při přihlášení/odhlášení včetně zaznamenání timestampu a zachycení HOSTNAME, IP stanice a spuštěného modulu SOS, se kterými uživatel provedl přihlášení/odhlášení. Každému uživateli v SOS jsou přiděleny role, podle nichž má oprávnění přístupu k datům a omezeny druhy manipulace s nimi.

Obdobným způsobem odpovídajícího přístupu v rámci IS operačního řízení je umožněn uživatelský přístup k dalším podpůrným IS, jde tedy o komunikaci uživatelů připojovaných zvenčí (WAN) a je dostatečně zabezpečena standardními prostředky zabezpečujícími VPN (virtuální privátní síť) připojení.

b) Logování činnosti

Činnost uživatelů a změny dat ze spolupracujících aplikací jsou logovány v logovacích tabulkách uložených v DB ORACLE, ze kterých je možné zpětně vyčíst druhy prováděných změn včetně času a uživatele/rozhraní, provádějícího danou změnu.

c) Omezení dat – validace

Celá řada údajů pořizovaných uživatelem v IS SOS je ochráněna a zabezpečena proti uživatelským nepřesnostem:

- parametrizovanou relační vaznou na definované číselníky;
- aplikačními omezeními (ochrana logických návazností, validace smysluplné časové posloupnosti jednotlivých fází řešení události).

Cílem těchto opatření je, aby uživatel nebyl schopen zadat nesprávná data, zároveň výskyt nesprávných dat je v aplikaci SOS doprovázen upozorněním na chybu v datech, aby mohl uživatel situaci vyhodnotit, a údaje správně opravit.

D. Ochrana (zabezpečení, uchování a zálohování) elektronických dat

➢ Ochrana dat IS OŘ ZOS – SOS

a) Technická bezpečnost

Bezpečnost dat pro použití v aplikaci systému operačního řízení ZOS SOS je zaručena na vysoké úrovni použitím kvalitní RDMBS ORACLE. Databázový systém ORACLE je špičkovým produktem v oblasti stability a robustnosti. Průkazným ukazatelem kvality a stabilnosti databázového systému ORACLE pro IS ZOS jsou i mnohaleté dobré zkušenosti s provozem tohoto informačního systému na DB ORACLE i v jiných ZZS v ČR. (NEWMAN a THERIAULT, 2004)

b) Zálohování dat ORACLE

Data uložená primárně v databázi ORACLE na serveru SOS1 jsou automaticky přírůstkově odlévána na záložní server SOS3 do databáze v off-line režimu, odkud je možno v případě výpadku SOS1 po aktualizaci-synchronizaci dat (dohrání posledních přírůstků) převést do on-line režimu a celou aplikaci SOS provozovat ze serveru SOS3, do doby, než bude opět zprovozněna databáze na SOS1, a převedena na ni nová aktuální data ze SOS3.

Pravidelné zálohy databáze IS SOS jsou pořizovány za provozu a nemají žádný vliv na kvalitu služeb poskytovaných systémem.

➢ Ochrana dat integrované hlasové komunikace

Oprávnění k přístupu k datům jsou řešena na úrovni standardních ACL seznamů souborového systému NTFS ve spojení s Active Directory doménou spravovanou ZZS. Subsystém integrace ukládá:

- provozní a ladicí protokoly (metadata) o voláních jednotlivými komunikačními prostředky;
- hovorová data krátkodobého záznamu s připojenými identifikačními údaji protistrany.

K vlastním záznamům má plný přístup obsluha dispečinku. Mimo tyto krátkodobé záznamy je pořizován záznam komunikace a to jak radiové, tak telefonní na samostatný systém ReDat, což je aplikační server fi. RETIA.

- **Ochrana dat MZD**

Ochrana dat u aplikace mobilního zadávání dat je zabezpečena proti jejich zneužití následovně:

- data přenášená z terénu pomocí tabletů přes GSM síť jsou šifrována (je možné využít jak veřejný internet, tak privátní APN);
- přístup na veřejně dostupné servery (eHealth konektory) je auditován a chráněn samostatnou autentizací aplikace;
- přístup na webové aplikace systému je umožněn pouze z vnitřní sítě koncového uživatele.

Přístup k vlastním datům pacienta je navíc zabezpečen:

- Přístup k datům je řešen oprávněním uživatelů (jméno a heslo).
- Uživatelské účty lze spravovat aplikacemi systému nebo možnou integrací na AD (**A**ctive **D**irectory).
- Vlastní přístup je auditován do samostatné tabulky.
- Granularita přístupu k jednotlivým datům je řešena uživatelskými právy.

5 Diskuze

Tato část bakalářské práce posuzuje stávající zjištěná opatření, ať už v rámci „klasických“ či „novodobých hrozeb, s jejich reálnou potřebou. V případě, že současná opatření jsou vyhodnocena jako nedostačující, jsou následně navrženy jejich úpravy či jejich doplnění o zcela úplně nová.

5.1 Posouzení efektivnosti současných opatření

V první části „Diskuze“ jsou posuzovány opatření v rámci nejčastějších, resp. nejpravděpodobnějších z tzv. „klasických hrozeb“ vycházejících z analýzy rizik. Jedná se o **výpadek dodávky el. energie**, **požár budovy a opatření v rámci PO**, **evakuační opatření v rámci hrozící MU** a **epidemie mezi zaměstnanci ZOS**.

5.1.1 Výpadek dodávky energie

Realizovanými opatřeními je budova z pohledu dodávek el. proudu soběstačná, což bylo i několikrát prověřeno zkušebním provozem. Jsou nastaveny i mechanismy zásobování, úhrady a skladování PHM, dieselagregát prochází pravidelnými kontrolami a atesty.

5.1.2 Požár budovy, opatření PO

Jelikož posuzovaný objekt je novostavba, odpovídá protipožární řešení nejnovějším trendům a předpisům PO. Tomu odpovídá i osazení všech dveří tzv. bezpečnostním kováním. Toto dovoluje otevření i zamčených dveří, které je samozřejmě možné výhradně ve směru ven z budovy, tedy ve směru evakuační cesty. Tímto opatřením je zcela eliminováno nebezpečí, že by zamčené dveře bránily v evakuaci a „uvěznily“ tak prchající zaměstnance v místě nebezpečí. Dále rozmístění požárních čidel v celém objektu je dnes již standardním opatřením, garáže jsou osazeny i senzory koncentrace výfukových plynů. Kladně je třeba hodnotit důraz na školení zaměstnanců,

které se opravdu provádí v předepsaném rozsahu a minimálně 1x ročně. Lokalizaci vzniklého požáru může odhalit nejen požární signalizace, ale i kamerový systém (venkovní, okolo celé budovy včetně vstupů, vnitřní pak v garážích), kterým je budova z důvodu bezpečnosti vybavena. Vizualizace obrazu kamerového systému je na pracovišti ZOS.

5.1.3 Evakuace ZOS z důvodu hrozící MU

V současné době je fungování chodu ZOS zajištěno velice efektivně, s minimálními časovými prodlevami při nutnosti evakuace tohoto pracoviště. Vstup do budovy, zajištěný elektronickým karetním systémem, odpovídá požadavkům na zajištění bezpečnosti, zamezující nekontrolovanému pohybu osob po budově, popř. kolem budovy, která je zvnějšku monitorována kamerovým systémem. Vstup na ZOS, jako na režimové pracoviště, je jištěn ještě jedním okruhem.

V současné době je v řešení technické dovybavení záložního pracoviště ZOS, včetně přenosu a uchovávání elektronických dat. Po případném naplnění nové koncepce bude následovat prověřovací fáze ke zjištění plné funkčnosti záložních systémů.

5.1.4 Epidemie mezi zaměstnanci

Poskytovatel PNP se snaží známá rizika eliminovat vzájemnou zastupitelností členů výjezdových skupin a operátorů ZOS. Velký důraz je kladen na prevenci. Vybavení sanitních vozů protiinfekčními balíčky je dobrým preventivním opatřením za minimální investici. Každý člen výjezdové skupiny ZZS PK musí být navíc povinně očkován proti hepatitidě A i B, další očkování jsou nepovinná (např. vakcinace sezónním kmenem chřipky či pandemickým kmenem). Lepší proočkovanost lze dosáhnout nejen osvětou, ale i finanční participací zaměstnavatele na nákladech za očkovací látku.

Nedílnou součástí připravenosti na tyto MU či KS jsou zpracované plány jako pandemický plán kraje, hygienicko-epidemiologický řád organizace a vnitřní

předpisy týkající se chodu zmíněného BHT. Určité části těchto plánů jsou rozpracovány v plánu krizové připravenosti s následným odkazem na ně.

5.2 Posouzení kybernetické bezpečnosti, návrh na její doplnění

Pro větší zabezpečení dat operačního řízení je možné striktně oddělit VLAN operačního řízení od ostatní komunikace přídavným bezpečnostním prvkem typu **FireWall** (centrální FireWall) **s modulem IPS ((Intrusion Prevention Systems – systém prevence průniku)** a tím omezit na maximum komunikaci z ostatních segmentů WAN sítě ZZS na pouze potřebnou komunikaci. Vzhledem k charakteru komunikace jednotlivých systémů jak v rámci WAN sítě, tak i sítí Internet a ITS nemůže být tato plně oddělena a samostatná.

Vhodným bezpečnostním prvkem je systém **SIEM (Security Information and Event Management)**, což je management bezpečnostních informací a událostí, který umožňuje agregovat, a korelovat bezpečnostní informace z různých zdrojů (FireWall, Server, Switch, Aplikace apod.) a varovat zaměstnance IT o hrozbách v rámci infrastruktury.

Existuje i **aplikační nadstavba na systém OŘ**, která umožňuje korelovat data z aplikace SOS s běžnými hrozbami v rámci infrastruktury. Předpokládá se i rozšíření auditu aplikace operačního řízení o bezpečnostní data o přístupu k osobním údajům, specifickým datům operačního řízení.

Pro zabezpečení interních sítí je možné také implementovat **technologii „port autentizaci“ 802.1X**. Jedná se tedy o kontrolu připojení autorizovaných zařízení v rámci WAN sítě ZZS a to jak prostřednictvím fyzického kabelu, tak i prostřednictvím bezdrátových sítí WiFi.

U aplikace MZD lze navíc šifrovaná data přenášet i pomocí sítě Wifi, tedy nejen sítí GSM z terénu. Hardwarová infrastruktura je na jednotlivých výjezdových základnách připravena, ale doposud nebylo toto řešení realizováno.

5.3 Odpověď na výzkumnou otázku

Odpověď na výzkumnou otázku zní: „Současný stav krizové připravenosti, resp. ochrany prvku kritické infrastruktury – zdravotnického operačního střediska ZZS Plzeňského kraje je dostačující a splňující všechny současně platné právní normy.“

6 Závěr

V současné době stávající zabezpečení zdravotnického operačního střediska ZZS Plzeňského kraje plně odpovídá standardům a všem povinnostem vyplývajícím z dosavadních právních norem.

Ve světle nových trendů však bude nutné zabezpečit tento prvek kritické infrastruktury více po stránce kybernetické bezpečnosti, byť v současné době tento prvek KI nespadá pod problematiku kybernetického zákona. K tomuto závěru nás vede jak stávající stav, tak celosvětový vývoj s meziročním nárůstem kybernetických incidentů.

Dalším krokem ke zvýšení krizové připravenosti ZZS Plzeňského kraje jako poskytovatele zdravotních služeb a zároveň základní složky IZS bude pořízení a dovybavení ICT pro případ evakuace stávajícího ZOS a tím zprovoznění dočasného – provizorního ZOS ve vytipovaných nasmlouvaných lokalitách.

Nedílnou součástí je sledování nových trendů ve vývoji informačních technologií, jejich pořizování, zároveň zvyšování erudice servisních IT zaměstnanců ZZS, ale i pravidelné proškolování zaměstnanců z řad operátorů ZOS a výjezdových skupin na bázi uživatelské.

Seznam použitých zdrojů

BRYLA Bob, LONEY Kevin, Mistrovství v Oracle Database 11g, Computer Press 2009, EAN 9788025121894, ISBN 978-80-251-2189-4

ČESKÁ ASOCIACE BEZPEČNOSTNÍCH MANAŽERŮ ve spolupráci s Ministerstvem vnitra – Generálním ředitelstvím Hasičského záchranného sboru, Ochrana kritické infrastruktury, monografie, Praha 2011, ISBN 978-80-260-1215-3

EICHLER, J. Terorismus a války v době globalizace. Praha: Karolinum, 2010, ISBN 978- 80-246-1790-9

Evropská směrnice 2008/114/ES, Směrnice Rady o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu, v úplném znění. R. 2008, částka L345, strana 75 - 82. Dostupné z www.hzscr.cz/soubor/smernice-eki-pdf.aspx

KHEILOVÁ, BOZPO Plzeň, s.r.o., dokumentace ZZS Plzeňského kraje (S – 43/2014) – Požárně poplachová směrnice, zpracovatel František Kheil OZO v oboru PO (Z-OZO-57/2007)

KHEILOVÁ, BOZPO Plzeň, s.r.o., dokumentace ZZS Plzeňského kraje (S – 42/2014) – Požární řád venkovního uzavřeného skladu tlakových lahví s kyslíkem, zpracovatel František Kheil OZO v oboru PO (Z-OZO-57/2007)

KHEILOVÁ, BOZPO Plzeň, s.r.o., dokumentace ZZS Plzeňského kraje (S – 41/2014) – Prohlášení o začlenění do kategorií podle míry požárního nebezpečí, zpracovatel František Kheil OZO v oboru PO (Z-OZO-57/2007)

KHEILOVÁ, BOZPO Plzeň, s.r.o., dokumentace ZZS Plzeňského kraje (S – 45/2014) – Řád ohlašovny požáru, zpracovatel František Kheil OZO v oboru PO (Z-OZO-57/2007)

KHEILOVÁ, BOZPO Plzeň, s.r.o., dokumentace ZZS Plzeňského kraje (S – 40-60/2014) - Směrnice pro BOZP a PO, zpracovatel František Kheil OZO v oboru PO (Z-OZO-57/2007)

KHEILOVÁ, BOZPO Plzeň, s.r.o., dokumentace ZZS Plzeňského kraje (S – 40/2014) – Školení PO, zpracovatel František Kheil OZO v oboru PO (Z-OZO-57/2007)

KUROSE F. James, ROSS W. Keith, Počítačové sítě, Computer Press 2014, EAN 9788025138250, ISBN 978-80-251-3825-0

NEWMAN Aaron, THERIAULT Marlene, Bezpečnost v Oracle, Computer Press 2004, EAN 9788072269792, ISBN 80-7226-979-8

Nařízení vlády č. 462/2000 Sb., k provedení § 27 odst. 8 a § 28 odst. 5 zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), 2000. In: *Sbírka zákonů České republiky*, částka 132, strana 7200 - 7211.

Nařízení vlády č. 432/2010 Sb. o kritériích pro určení prvku kritické infrastruktury, 2010. In: *Sbírka zákonů České republiky*, částka 149, strana 5623 - 5630. ISSN 1211-1244

Nařízení vlády č. 315/2014 Sb., kterým se mění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, 2014. In: *Sbírka zákonů České republiky*, částka 127, strana 3964 - 3971. ISSN 1211-1244

NBÚ – NCKB, Metodická příručka se základními informacemi a průvodcem pro určování KII / VIS, Praha 2015, verze 3 z 5. 8. 2015

Opatření obecné povahy vydané Ministerstvem vnitra České republiky pod čj. MV-55222-2/PO-OKR-2012, MV ČR 11. 6. 2012

PER4MANCE s.r.o., Systémová dokumentace k IOP 11 (2010), upgrade 2017

RUEST Danielle and RUEST Nelson, Virtualizace - podrobný průvodce, Computer Press 2010, EAN 9788025126769, ISBN 978-80-251-2676-9

STANEK R. Wiliam, Microsoft Windows Server 2012 - kapesní rádce administrátora, Computer Press 2015, EAN 9788025138175, ISBN 978-80-251-3817-5

STREBE Matthew, PERKINS Charles, Firewally a proxy-servery, Computer Press 2003, EAN 9788072269839, ISBN 80-7226-983-6

ŠENOVSKÝ Michail, ADAMEC Vilém, ŠENOVSKÝ Pavel, Ochrana kritické infrastruktury, Edice SPBI Spektrum 2007, ISBN: 978-80-73850-25-8

ŠIKA Michal, 333 tipů a triků pro VMware, Computer Press 2012, EAN 9788025136591, ISBN 978-80-251-3659-1

ŠTOREK Josef, Krizový management, krizová připravenost, medicína katastrof, KARTPRINT, Bratislava 2015, ISBN 978-80-89553-31-0

Tisková zpráva MZV ČR, 31. 1. 2017 [online]. Ministerstvo zahraničních věcí České republiky [cit. 2017-03-08]. Dostupné z http://www.mzv.cz/jnp/cz/udalosti_a_media/tiskove_zpravy/x2017_01_31_mzv_celilo_kyberutokum.html

Tisková zpráva MZ ČR, 10. 1. 2017 [online]. Ministerstvo zdravotnictví České republiky [cit. 2017-03-10]. Dostupné z http://www.mzcr.cz/dokumenty/ptaci-chripka-a-jeji-rizika_13248_1.html

Vyhláška Ministerstva vnitra č. 246/2001 Sb. o stanovení podmínek požární bezpečnosti a výkonu státního požárního dozoru (vyhláška o požární prevenci), 2001. In: *Sbírka zákonů České republiky*, částka 95, strana 5446 - 5489.

Vyhláška Ministerstva zdravotnictví č. 240/2012 Sb., kterou se provádí zákon o zdravotnické záchranné službě, 2012. In: *Sbírka zákonů České republiky*, částka 82, strana 3226 - 3231. ISSN 1211-1244

Vyhláška NBÚ č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti), kterou se provádí zákon č. 181/2014 Sb. o kybernetické bezpečnosti, 2014. In: *Sbírka zákonů České republiky*, částka 127, strana 3972 - 4006. ISSN 1211-1244

Vyhláška NBÚ a Ministerstva vnitra č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, 2014. In: *Sbírka zákonů České republiky*, částka 127, strana 4007 - 4013. ISSN 1211-1244

WEDOS Internet, a.s. [online], Co je virtualizace? [cit. 2017-03-15]. Dostupné z *https://hosting.wedos.com/cs/virtual/co-je.html*

Zákon České národní rady č. 133/1985 Sb. o požární ochraně, ve znění pozdějších předpisů, 1985. In: *Sbírka zákonů České republiky*, částka 34, strana 674 - 691.

Zákon č. 239/2000 Sb. o integrovaném záchranném systému a o změně některých zákonů, 2000. In: *Sbírka zákonů České republiky*, částka 73, strana 3461 - 3474.

Zákon č. 240/2000 Sb. o krizovém řízení a změně některých zákonů (krizový zákon), 2000. In: *Sbírka zákonů České republiky,* částka 73, strana 3475 - 3487.

Zákon č. 372/2011 Sb. o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách), 2011. In: *Sbírka zákonů České republiky,* částka 131, strana 4730 - 4801. ISSN 1211-1244

Zákon č. 374/2011 Sb. o zdravotnické záchranné službě, 2011. In: Sbírka zákonů České republiky, částka 131, strana 4839 - 4848. ISSN 1211-1244

Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), 2014. In: Sbírka zákonů České republiky, částka 75, strana 1926 - 1936. ISSN 1211-1244

Zřizovací listina Zdravotnické záchranné služby Plzeňského kraje ze dne 15. 4. 2003, zapsanou v obchodním rejstříku u Krajského soudu v Plzni, pod spisovou zn. Pr 684. Dostupné z https://or.justice.cz/ias/ui/rejstrik-$firma?ico=45333009

ZZS Plzeňského kraje, vnitřní předpisy organizace – Hygienicko-epidemiologický řád ZZS PK, Plzeň 2016

ZZS Plzeňského kraje, vnitřní předpisy organizace – Organizačně provozní řád zdravotnického operačního střediska, Plzeň 2017

ZZS Plzeňského kraje, vnitřní předpisy organizace – Organizační řád, Plzeň 2016

ZZS Plzeňského kraje, vnitřní předpisy organizace – Plán krizové připravenosti, Plán krizové připravenosti subjektu kritické infrastruktury, Plzeň 2017

Seznam zkratek

ACL	**A**ccess **C**ontrol **L**ist (seznam pro řízení přístupu)
AČR	Armáda České republiky
AD	**A**ctive **D**irectory
ADSL	**A**symmetric **D**igital **S**ubscriber **L**ine
angl.	anglický, z angličtiny
APN	**A**ccess **P**oint **N**ame (jméno přístupového bodu)
ARPA	**A**dvanced **R**esearch **P**rojects **A**gency
BHT	**B**io **H**azard **T**eam
BSL	**B**io**S**afety **L**evel (stupeň biologické bezpečnosti)
BOZP	bezpečnost a ochrana zdraví při práci
CBO	centrum biologické ochrany
CLZS	centrum letecké záchranné služby
ČSN	dříve **Č**eskoslovenská **s**tátní **n**orma, dnes neofic. **Č**eská **s**oustava **n**orem, resp. České technické normy
ČR	Česká republika
ČSFR	Česká a Slovenská federativní republika
čj.	číslo jednací
ČVUT	České vysoké učení technické
DB	databáze
DSL	**D**igital **S**ubscriber **L**ine
EAN	**E**uropean **A**rticle **N**umber (evropské číslo obchodní položky)

EKI	evropská kritická infrastruktura
EKP	elektronická karta pacienta
EMS	**E**mergency **H**ealth **S**ervice
EPS	elektrická požární signalizace
ES	evropská směrnice
franc.	francouzský, z francouzštiny
Gbps	**G**iga**b**it **p**er **s**ecundam (Gigabit za sekundu)
GIS	**G**eographic **I**nformation **S**ystem (geografický informační systém)
GSM	**g**lobální **s**ystém pro **m**obilní komunikaci (z franc. „Groupe Spécial Mobile“)
GŘ	generální ředitelství
HPO	hromadné postižení osob
HW	hardware
HZS	hasičský záchranný sbor
HZS PK	Hasičský záchranný sbor Plzeňského kraje
IBM	**I**nternational **B**usiness **M**achines Corporation
ICS	**I**ndustrial **C**ontrol **S**ystem (průmyslový řídící systém)
ICT	**I**nformation and **C**ommunication **T**echnologies (informační a komunikační technologie)
iDRAC7	**I**ntegrated **D**ell **R**emote **A**ccess **C**ontroller **7**
Inc.	Incorporated (am. zapsaný v obchodním rejstříku)
IOS	integrované operační středisko
iROP	integrovaný regionální operační program

ISBN	**I**nternational **S**tandard **B**ook **N**umber (mezinárodní standardní číslo knihy)
iSCSI	**I**nternet **S**mall **C**omputer **S**ystem **I**nterface (síťový protokol)
ISSN	**I**nternational **S**tandard **S**erial **N**umber (mezinárodní standardní číslo seriálové publikace)
IP	**I**nternet **P**rotocol
IPS	**I**ntrusion **P**revention **S**ystems (systém prevence průniku)
IS	informační systém
ISDN	**I**ntegrated **S**ervices **D**igital **N**etwork (digitální síť integrovaných služeb)
ISMS	**I**nformation **S**ecurity **M**anagement **S**ystem (systém řízení bezpečnosti informací)
ISVS	informační systémy veřejné správy
IT	**I**nformation **T**echnologies (informační technologie)
ITS	integrovaná telekomunikační síť
ITS MV ČR	integrovaná telekomunikační síť Ministerstva vnitra České republiky
IZS	integrovaný záchranný systém
KB	kybernetická bezpečnost
KI	kritická infrastruktura
KII	kritická informační infrastruktura
KOPIS	krajské operační a informační středisko
KP	krizový plán
KŘ	krajské ředitelství
KŘP	krajské ředitelství policie
KŘP PK	Krajské ředitelství policie Plzeňského kraje

KS	komunikační systém
KS	krizová situace
KÚ PK	Krajský úřad Plzeňského kraje
LAN	**L**ocal **A**rea **N**etwork (lokální síť, místní síť)
LCT	**L**anguage and **C**ommunication **T**echnologies (jazykové a komunikační technologie)
LZS	letecká záchranná služba
MERS	**M**iddle **E**ast **R**espiratory **S**yndrome (Blízkovýchodní respirační syndrom)
min.	minuta
MU	mimořádná událost
MU s HPO	mimořádná událost s hromadným postižením osob
MV	ministerstvo vnitra
MV ČR	Ministerstvo vnitra České republiky
MZ	ministerstvo zdravotnictví
MZ ČR	Ministerstvo zdravotnictví České republiky
MZD	mobilní zadávání dat
MZV	ministerstvo zahraničních věcí
MZV ČR	Ministerstvo zahraničních věcí České republiky
NBÚ	Národní bezpečnostní úřad
NCKB	Národní centrum kybernetické bezpečnosti
NDIC	Národní dopravní informační centrum
NIS	**N**etwork **I**nformation **S**ervice (servisní informační síť)
NPZ	nahodilé požární zatížení

NTFS	**N**ew **T**echnology **F**ile **S**ystem (souborový systém)
NV	nařízení vlády
OLZS a UM	Odbor letecké záchranné služby a urgentní medicíny Armády ČR
OOP	opatření obecné povahy
OOPP	osobní ochranné pracovní pomůcky
OŘ	operační řízení
OS	operační systém
OVM	orgán veřejné moci
OZO	odborně způsobilá osoba
PAT	**P**ort **A**dress **T**ranslation
PC	**P**ersonal **C**omputer (osobní počítač)
PBŘ	požárně bezpečnostní řešení
PCoIP	PC-over-IP
PČR	Policie České republiky
PHM	pohonné hmoty
PK	Plzeňský kraj
PKI	prvek kritické infrastruktury
PKP	plán krizové připravenosti
PNP	přednemocniční neodkladná péče
PO	požární ochrana
PP	podzemní podlaží
PS	požární stanice
PPP	preventivní požární prohlídka

PPS	požární poplachová směrnice
RÚIAN	Registr územní identifikace, adres a nemovitostí
SAN	**S**torage **A**rea **N**etwork (dedikovaná oddělená síť od LAN, WAN, atd.)
SARS	**S**evere **A**cute **R**espiratory **S**yndrome (syndrom těžkého akutního respiračního selhání)
SCADA	**S**upervisory **C**ontrol **A**nd **D**ata **A**cquisition (≈ dispečerské řízení a sběr dat)
SIEM	**S**ecurity **I**nformation and **E**vent **M**anagement (management bezpečnostních informací a událostí)
SPD	státní požární dozor
SMS	**S**hort **M**essage **S**ervice (služba krátkých textových zpráv)
SW	software
TCTV	telefonické centrum tísňového volání
THP	technicko - hospodářský pracovník
TS	tisková zpráva
UPS	**U**ninterruptible **P**ower **S**upply/**S**ource (zdroj nepřerušovaného napájení)
ÚSZS	Územní středisko záchranné služby
VDSL	**V**ery Speed **DSL**
VHDSL	**V**ery **H**igh Speed **DSL**
VIS	významný informační systém
VKB	vyhláška o kybernetické bezpečnosti
VLAN	**V**irtual **LAN** (virtuální lokální síť)
VM	**V**irtual **M**achine (virtuální stroj)
VNN	vysoce nakažlivá nemoc

VPN	vysoké požární nebezpečí
VPN	**V**irtual **P**rivate **N**etwork (virtuální privátní síť)
VZ	výjezdová základna
WAN	**W**ide **A**rea **N**etwork (rozsáhlá síť)
WLAN	**W**ireless **LAN** (bezdrátová lokální síť)
WS	webové služby
WWW	**W**orld **W**ide **W**eb (zkráceně **web**)
ZOS	zdravotnické operační středisko
ZDS	zdravotní dopravní služba
ZKB	zákon o kybernetické bezpečnosti
ZPN	zvýšené požární nebezpečí
ZZS	zdravotnická záchranná služba
ZZS PK	Zdravotnická záchranná služba Plzeňského kraje

Seznam obrázků

Obrázek 1 – Budova ředitelství, ZOS a VZ Plzeň-Bory

Obrázek 2 – Generátor elektrického proudu (zdroj: archív ZZS PK)

Obrázek 3 – Piktogram úniková cesta

Obrázek 4 – Piktogram únikový východ

Obrázek 5 – Bio Hazard Team na výcviku v CBO Těchonín

Obrázek 6 – Znázornění fyzické architektury serverového systému ZOS

Obrázek 7 – HW serverová infratruktura ZOS

Obrázek 8 – Datové úložiště DELL EqualLogic řady PS6110 10 Gbps iSCSI s redundantními řadiči

Obrázek 9 – Dispečerské pracoviště na ZOS

Obrázek 10 – Schéma klasického serveru a serveru s virtualizační vrstvou

Seznam příloh

Příloha A Prohlášení o začlenění do kategorií podle míry požárního nebezpečí u ZZS Plzeňského kraje

Příloha B Požární řád pro činnost ZPN ve skladu O_2 ZZS Plzeňského kraje

Příloha C Požární poplachové směrnice ZZS Plzeňského kraje

Příloha D Řád ohlašovny požáru ZZS Plzeňského kraje

Příloha E Příklad zpracování osnov tematických plánů u ZZS Plzeňského kraje

Příloha F Evakuační plán 1. PP (dílny), dokumentace PO ZZS Plzeňského kraje

Příloha G Evakuační plán 1. PP (garáže), dokumentace PO ZZS Plzeňského kraje

Příloha H Evakuační plán 1. NP, dokumentace PO ZZS Plzeňského kraje

Příloha CH Evakuační plán 2. PP, dokumentace PO ZZS Plzeňského kraje

Příloha I Porovnání únikových tras

Příloha A **Prohlášení o začlenění do kategorií podle míry požárního nebezpečí u ZZS Plzeňského kraje**

(dokumentace PO ZZS PK – zpracovatel František Kheil OZO v oboru PO (Z-OZO-57/2007))

Prohlášení o začlenění do kategorií podle míry požárního nebezpečí

Zpracováno na základě znění § 28 vyhlášky MV č. 246/2001 Sb., kterou se provádějí některá ustanovení zákona o PO.

Organizace: **Zdravotnická záchranná služba Plzeňského kraje**						**Zpracoval**: OZO - František Kheil – Z-OZO-57/2007
Část II. - ČINNOST SE ZVÝŠENÝM POŽÁRNÍM NEBEZPEČÍM						
Druh provozované činnosti	Místo provozované činnosti	Hořlavá/hoření podporující látka	Množství používané hořlavé látky	Počet zaměstnanců trvale	Hodnota p^n kg/m² / Vyhl. 246/01 Sb.	Charakteristika činnosti se zvýšeným požárním nebezpečím zákon o PO § 4 odst. 2 písm. :
SKLADOVÁNÍ KYSLÍKU	**areál ZZS Pk** Klatovská třída 2960/200i 301 00 Plzeň místnost – 029 PÚ – 01.13	kyslík - O_2 max. 2500litrů pro potřeby ZZS max. 200 ks láhví á10litrů a 25 ks láhví á 2 litry	max. 2500litrů pro potřeby ZZS max. 200 ks láhví á10litrů a 25 ks láhví á 2 litry	0	180 / §19 pol. 10.6	b) v jednom požárním úseku se vyskytují hoření podporující plyny o objemu nádob převyšujícím 100 litrů
OPRAVY VOZIDEL VLASTNÍHO VOZOVÉHO PARKU S PŘÍRUČNÍM SKLADEM PNEUMATIK	**autodílna 1PP ZZS Pk** Klatovská třída 2960/200i 301 00 Plzeň místnost – 010,012 PÚ – 01.2	Pneumatiky max.50 litrů acetylenu max.50 litrů kyslíku	max. 150kg/m² 50 litrů acetylenu 50 litrů kyslíku	3	150 / pol. 10.5	e) v prostoru se vyskytuje nahodilé požární zatížení vyšší než 120 kg/m² f) v prostoru se používá otevřený oheň v bezprostřední přítomnosti hořlavých látek v pevném, kapalném nebo plynném stavu
HROMADNÁ GARÁŽ -15 SANITNÍCH VOZŮ	**budova 1PP ZZS Pk** Klatovská třída 2960/200i 301 00 Plzeň místnost – 011 PÚ – 01.1	kyslík - O_2 30 ks láhví á10litrů 30 ks láhví á 2 litry *Počítáno při garážování velkých vozidel*	dohromady 360 litrů hoření podporujících plynů	0	180 / §19 pol. 10.6	b) v jednom požárním úseku se vyskytují hoření podporující plyny o objemu nádob převyšujícím 100 litrů

Příloha B Požární řád pro činnost ZPN ve skladu O_2 ZZS Plzeňského kraje

(dokumentace PO ZZS PK – zpracovatel František Kheil OZO v oboru PO (Z-OZO-57/2007)

Požární řád

venkovního uzavřeného skladu tlakových lahví s kyslíkem O_2

upravuje základní zásady zabezpečování PO na pracovišti

Klatovská třída 2960/200i, 301 00 Plzeň

Tento požární řád je interním právním předpisem, který je zpracován na podkladě znění § 31 vyhlášky MV č. 246/2001 Sb., kterou se provádějí některá ustanovení zákona ČNR o PO.

I.
STRUČNÝ POPIS VYKONÁVANÉ ČINNOSTI

Ve skladu (uzavřený sklad) jsou uloženy prázdné a plné tlakové láhve s medicinálním kyslíkem, které jsou používány ve vozidlech zdravotnické záchranné služby.
Sklad se nachází z přední strany budovy (příjezdové cesty).
Požární nebezpečí: v prostoru se vyskytují hoření podporující plyny v množství přesahujícím 100 litrů.

II.
CHARAKTERISTIKA LÁTEK

Medicinální kyslík je bezbarvý plyn, bez zápachu, který sám nehoří. Již při mírně zvýšené koncentraci zvyšuje intenzitu hoření látek, které jsou v normálním prostředí atmosféry nehořlavé. Ve velmi silné koncentraci je schopen vytvářet s organickými látkami, oleji a jinými mastnými látkami výbušnou směs. Kyslík má hustotu při 0^0C 1,429 kg m^{-3}a hustotu par vztažených na vzduch 1,1. Vzhledem k této skutečnosti bude při náhodných únicích klesat k zemi.
Požárně-technická charakteristika je součástí „Podmínek požární bezpečnosti"

III.
NEJVÝŠE PŘÍPUSTNÉ MNOŽSTVÍ LÁTEK

Dle ČSN 07 8304 jde o malý sklad nádob do 50 lahví plných nebo prázdných s vnitřním objemem do 50 litrů (samostatný požární úsek PÚ-01.13).

Skladování povoleno celkem do 2500 litrů

Pro potřeby organizace jsou využity pouze láhve s vnitřním objemem á10litrů a á2 litry.

Kyslík (O_2) - max. 200 ks á 10 litrů
- max. 25 ks á 2 litry

IV.
PODMÍNKY POŽÁRNÍ BEZPEČNOSTI K ZAMEZENÍ VZNIKU A ŠÍŘENÍ POŽÁRU

- Skladování lahví je přípustné pouze svislé poloze, láhve musí být zajištěny proti pádu!
- Je zakázáno vyprazdňovat tlakové láhve přímým ohříváním!
- Každý kdo vstoupí do skladu je povinen počínat si tak, aby svým jednáním nezpůsobil vznik požáru!
- Všichni zaměstnanci jsou povinni udržovat únikové cesty stále volné, nezastavené!
- Ve skladu medicinálních plynů nesmí být skladován materiál, který nesouvisí s provozem
- V okruhu 10m od skladu se nesmí kouřit ani manipulovat s otevřeným ohněm a nesmí zde být ukládány žádné hořlavé látky.
- Ve skladu a jeho okolí platí přísný zákaz kouření a vstupu s otevřeným ohněm!
- Do skladu je zakázáno donášet hořlavé látky, zapalovače a mobilní telefony.
- Sklad musí být označen výstražnými tabulkami: „ZÁKAZ KOUŘENÍ A MANIPULACE S OTEVŘENÝM OHNĚM", označení skladovaného plynu a „ZÁKAZ VSTUPU NEPOVOLANÝM OSOBÁM".
- Prázdné a plné lahve musí být uloženy odděleně a označeny tabulkami „PLNÉ LAHVE" a „PRÁZDNÉ LAHVE"!
- Poškozené nebo unikající tlakové láhve musí být uloženy do vyhrazeného prostoru, který musí být označen „Vadné láhve"!
- Vozidla přijíždějící na nakládku a vykládku technických plynů musí mít při manipulaci s tlakovými lahvemi vypnutý motor!
- Sklad musí být chráněn před účinky atmosférické elektřiny (pospojení, uzemnění)!

Příloha B (pokračování)

- Povrchová teplota lahví nesmí překročit 40°C!
- Ventily tlakových lahví musí být řádně uzavřeny!
- Kyslíkové lahve nesmějí přijít do styku s mastnotou!
- Skříň musí být mimo dobu manipulace (zaskladňování /vyskladňování) s lahvemi uzamčena!
- **Veškeré práce**, které se provádějí **pomocí otevřeného ohně**, se mohou provádět pouze po stanovení a vyhodnocení možného požárního nebezpečí a **vystavení požárně bezpečnostních opatření** (písemný příkaz) s vymezenou dobou platnosti a následného dozoru po ukončení práce. Změní-li se podmínky požární bezpečnosti v průběhu svařování, lze v něm pokračovat až po novém vyhodnocení a zajištění požárně bezpečnostních opatření. (viz vyhl. č. 87/2000 Sb. – podmínky požární bezpečnosti při svařování).
- Drobné opravy a údržbu zařízení mohou zaměstnanci provádět pouze na příkaz vedení organizace

V.
OPRÁVNĚNÍ A POVINNOSTI OSOB PŘI ZAJIŠŤOVÁNÍ POŽÁRNÍ BEZPEČNOSTI

- Bezpečnostní opatření pro práce pomocí otevřeného ohně vydává před zahájením prací – vedení ZZS / OZO v oboru PO – technik PO.
- Příslušní vedoucí zaměstnanci a fa, zajišťující dodavatelsky požární ochranu je povinna dohlížet na dodržování požární bezpečnosti při skladování.

VI.
PODMÍNKY PRO BEZPEČNÝ POBYT A POHYB OSOB

- Všichni zaměstnanci, kteří se zdržují v prostoru skladu nebo v něm manipulují s tlakovými lahvemi jsou povinni dodržovat tento požární řád.
- Přenosné hasící přístroje musí být trvale přístupné.
- Vedení ZZS je povinno kontrolovat své zaměstnance ve smyslu tohoto požárního řádu.
- **Všichni zaměstnanci jsou povinni upozorňovat na závady požární ochrany.**

Za požární ochranu odpovídá: ředitel organizace – MUDr. Roman Sviták

PŘÍLOHA požárního řádu

1. SEZNAM ČLENŮ PREVENTIVNÍ POŽÁRNÍ HLÍDKY PRACOVIŠTĚ A POKYNY PRO JEJÍ ČINNOST

PREVENTIVNÍ POŽÁRNÍ HLÍDKA NENÍ ZŘÍZENA - §13 ZÁKONA O PO / NA DANÉM PRACOVIŠTI NENÍ ZARUČENA STÁLÁ PŘÍTOMNOST MIN. TŘECH ZAMĚSTNANCŮ

2. VĚCNÉ PROSTŘEDKY A ZAŘÍZENÍ PO:

1x hasící přístroj sněhový S5 70B
1x vnější požární nadzemní hydrant DN 100 – vzdálenost od skladu 65metrů
1x Požární uzávěr otvorů – dveře EW 30DP3+C3
1x tlačítkový hlásič
1x optickokouřový hlásič
1x skříňka s OOPP, prostředky první pomoci a náhradními díly

3. BEZPEČNOSTNÍ A POŽÁRNÍ ZNAČKY:

„Kyslík" / max. počet lahví
„Zákaz kouření a manipulace s otevřeným ohněm v okruhu 10metrů"
„Zákaz vstupu nepovolaným osobám"
„Nebezpečí požáru a výbuchu" vstup do skladu
„Prázdné láhve" - „Plné láhve" - označení daného skladového prostoru
„Vadné láhve" - vymezený prostor
„Tlakové láhve" - vstup do skladu

V Plzni: **6. 6. 2014**

Schválili dne **6. 6. 2014**: **MUDr. Roman Sviták – ředitel organizace a zástupci OS**

Příloha C Požární poplachové směrnice ZZS Plzeňského kraje

(dokumentace PO ZZS PK – zpracovatel František Kheil OZO v oboru PO (Z-OZO-57/2007))

POŽÁRNÍ POPLACHOVÁ SMĚRNICE - vymezuje povinnosti zaměstnanců a zákazníků v případě požáru (VS Plzeň Bory)

POKYNY PŘI ZPOZOROVÁNÍ POŽÁRU

V případě vzniku požáru:

Požární poplach v objektu se vyhlašuje pomocí **EPS** nebo ručních tlačítkových spínačů pro spuštění **sirény** a voláním „**HOŘÍ**"!

Preventivní požární hlídka provede průzkum místa požáru a záchranu osob z ohrožených prostor! Je-li to možné, hasicími přístroji provede první zásah. NERISKUJTE!

Přivolejte jednotku HZS tel. číslo 150 nebo 112

Hlášení na ohlašovnu obsahuje:

1. kdo volá
2. objekt a rozsah požáru
3. přesná adresa
4. telefonní číslo odkud je voláno
5. upozornění na nejjednodušší příjezdovou trasu k požářišti

Vyčkejte zpětného dotazu jednotky HZS

Požár ohlaste vedení organizace a dispečinku ZOS (OHLAŠOVNA POŽÁRŮ) !!!!!!!

O požáru ihned informujte vedení organizace a Ohlašovnu požárů, která je zřízena v budově dispečinku.

Zahajte evakuaci osob a materiálu z ohrožených prostor – zejména tlakových lahví a sanitních vozidel, ve kterých jsou tlakové láhve s kyslíkem a připravte vše pro příjezd hasičského záchranného sboru (např. vypnutí HVE,...).

Osobní pomoc je Vaší zákonnou povinností! Po evakuaci a příjezdu záchranných jednotek oznamte hasičům všechny informace o místě a druhu požáru, umístění uzávěrů médií případně další důležité informace o zasaženém prostoru. Poskytněte pomoc postiženým nebo zraněným osobám.

112 INTEGROVANÝ ZÁCHRANNÝ SYSTÉM

HASIČI	150	Plyn	1239
ZÁCHRANKA	155	El. zař.	840 850 860
POLICIE	158	Voda	377 413 444
HASIČI SPD	950 330 111	Ohlašovna	377 672 111

Při volání z pevné linky z prostor organizace používejte před každým volaným číslem **0** !!!

POKYNY PRO EVAKUACI

V případě evakuace:

- Při opuštění evakuovaného prostoru zavřete (ale nezamykejte!) dveře a okna.
- Opusťte evakuovaný objekt nejkratší únikovou cestou.
- Při evakuaci zachovejte klid, neběhejte, nepanikařte, prostor opusťte rychlou chůzí
- Před otevřením dveří při úniku dotykem rukou zkontrolujte jejich teplotu. Pokud jsou dveře na dotyk horké, raději vyhledejte jinou únikovou cestu a upozorněte ostatní.
- Po opuštění evakuovaného objektu se dostavte na shromaždiště pro kontrolu počtu evakuovaných osob –před budovou VS – tak, abyste neztěžovali příjezd jednotek HZS.
- V případě, že není možné opustit objekt únikovými cestami:
  - zachovejte klid
  - v případě zakouření prostoru se přikrčte k zemi
  - upozorněte na sebe z okna – použijte ručník, část oděvu apod. nebo volejte 150/112 a oznamte svoji polohu
  - v žádném případě k evakuaci nepoužívejte výtah

TENTO VÝTAH NESLOUŽÍ K EVAKUACI OSOB

- Poskytněte veškeré informace o průběhu evakuace a dalších skutečnostech, které mohou pomoci, zásahovým jednotkám.

Po příjezdu Hasičského záchranného sboru se všichni zaměstnanci plně podřídí rozkazům velitele zásahu.

Zaměstnanci a požární hlídka se pokusí zajistit vypnutí el. energie, evakuaci tlakových lahví a hořlavých kapalin z prostor zasažených požárem.

HLAVNÍ UZÁVĚR VODY | HLAVNÍ VYPÍNAČ | TLAKOVÉ LÁHVE

Pro zpřístupnění celého objektu v případě HAVÁRIE je možno využití generálního klíče, který je uložen (zabezpečen) v prostoru dispečinku ZOS

Příloha D Řád ohlašovny požáru ZZS Plzeňského kraje

(dokumentace PO ZZS PK – zpracovatel František Kheil OZO v oboru PO (Z-OZO-57/2007))

Zdravotnická záchranná služba Plzeňského kraje, příspěvková organizace

ŘÁD OHLAŠOVNY POŽÁRŮ

vymezuje povinnosti zaměstnance, který přijímá hlášení o požáru

Klatovská třída 2960/200i, 301 00 Plzeň

1) Ohlašovna požáru je umístěna v "dispečinku ZOS" kde je zajištěna nepřetržitá služba 24 hodin denně.

2) Zaměstnanec, který přijímá hlášení o vzniku požáru zabezpečuje vyhlášení požárního poplachu, včetně oznámení požáru firmám jejichž pracoviště se nalézají v areálu. Poplach se vyhlašuje voláním "HOŘÍ" a „RUČNÍMI TLAČÍTKOVÝMI SPÍNAČI – EPS"!

3) Poté musí zaměstnanec vyrozumět **ústřednu ohlašovny požáru jednotky HZS Plzeňského kraje**

☎ 150 - **Hlášení na ohlašovnu obsahuje:**

a) kdo volá
b) objekt a rozsah požáru
c) přesná adresa
d) telefonní číslo odkud je voláno
e) upozornění na nejjednodušší příjezdovou trasu k požářišti

Zaměstnanec, který hlásí vznik požáru vyčká zpětného dotazu jednotky Hasičského záchranného sboru.

4) Do příjezdu jednotky vykoná / zajistí zaměstnanec dispečinku nezbytné přípravy pro zabezpečení snadného příjezdu na požářiště. Po příjezdu jednotky je nápomocen veliteli zasahující jednotky a podá mu náležité informace o areálu - objektu (přístupové komunikace, uložení generálního klíče, nebezpečné látky na požářišti, vypínače el. energie, hl. uzávěr vody a umístění požárních hydrantů)

Hasičský záchranný sbor (ohlašovna požárů) ☎ 150

SOS tísňové volání (Emergency call)..... ☎ 112

Ostatní důležitá telefonní čísla :

Zdravotní záchranná služba	**1 5 5**
Policie - tísňové volání	**1 5 8**
El proud - pohotovostní služby	**840 850 860**
Plyn - pohotovostní služby	**1239**
Voda - pohotovostní služby	**377 413 444**
Hasičský záchranný sbor, Kaplířova 9, Plzeň (SPD)	**950 330 111**
Policejní oddělení Plzeň, Družstevní 1851/16	**974 325 395**
Sousední objekt - SŠ informatiky a fin. služeb	**377 401 111**
Sousední objekt – POLICIE ČR	**1 5 8**

V Plzni: **6. 6. 2014**

Schválili dne **6. 6. 2014**: **MUDr. Roman Sviták – ředitel organizace a zástupci OS**

Příloha E Zpracování osnov tematických plánů u ZZS Plzeňského kraje

(dokumentace PO ZZS PK – zpracovatel František Kheil OZO v oboru PO (Z-OZO-57/2007))

Příloha č. 1

část I. – tématické plány školení určené vedoucím zaměstnancům - školení se provádí 1 x za 3 roky

1. Organizace a zajištění PO a základní povinnosti zaměstnanců vyplývající z předpisů o PO

a) Zákoník práce č. 262/2006 Sb.

- základní povinnosti vedoucích zaměstnanců - § 302
- povinnosti zaměstnavatele - § 103
- práva a povinnosti zaměstnanců - § 106,301

b) Zákon ČNR č. 133/1985 Sb. ve znění pozdějších změn a doplňků (úplné znění č. 67/01Sb)

- povinnosti právnických osob a podnikajících fyzických osob - §§ 2- 6
  zejména - § 4 – členění podle požárního nebezpečí
  §13 – preventivní požární hlídka
  §15 - dokumentace PO
  §16 - školení a odborná příprava zaměstnanců o požární ochraně
- státní správa na úseku PO - §§ 23 - 38
- jednotky PO - pouze informativně
- pokuty právnickým a podnikajícím fyzickým osobám - §§ 76 a 78

c) Vyhláška MV č. 246/2001 Sb.

- povinnosti právnických a podnikajících fyzických osob
  zejména - hasící přístroje - § 2,3
  dokumentace PO u právnických a podnikajících fyz. osob - § 27
  dokumentace o začlenění do kategorie činností - § 28
  požární kniha - § 37
  školení a odb. příprava zaměstnanců o požární ochraně - § 23, 24
- úkoly státních orgánů na úseku PO - §§ 45-50
  zejména - provádění kontrol SPD
- definice požáru

přednáška : 15 min.

2. Požární nebezpečí v objektech a při činnostech se zvýšeným požárním nebezpečím

- proces hoření - principy hašení
- preventivní požární hlídky - zákon § 13, činnost při požáru
- stručná charakteristika požárně nebezpečných látek vyskytujících se na pracovištích
- činnosti se zvýšeným požárním nebezpečím a zabezpečení pracovišť při těchto pracích
- PHP - vhodnost, pravidelné kontroly 1x za rok
- požární vodovody, použití, revize 1x za rok

přednáška : 15 min.

3. Dokumentace PO

vyhláška MV č. 246/2001 Sb.

- začlenění do kategorií
- směrnice PO
- požární řády - § 31+ seznámení se zněním požárního řádu
- požární poplachová směrnice - § 32 + seznámení se zněním požární poplachové směrnice
- tematické plány školení
- dokumentace o provedeném školení zaměstnanců a odborné přípravě preventivních požárních hlídek
- požární kniha
- Požární evakuační plán

přednáška : 30 min.

Příloha E (pokračování)

4. Seznámení s požadavky na provoz, údržbu a obsluhu zařízení v případě vzniku požáru

- rozmístění hl. uzávěrů vody, plynu a hl. vypínače el. proudu
- vyhlašování požárního poplachu - způsoby
- evakuace osob, materiálu a techniky - seznámení se způsoby
- zpřístupnění místa požáru pro zasahující jednotky PO
- § 18,19,20 zákona ČNR č.133/1985 Sb., v posledním úplném znění č. 67/2001 Sb. - osobní a věcná pomoc při zdolávání požáru

přednáška : 15 min.

5. Požadavky pro výkon požárně nebezpečných činností - technické normy a právní předpisy v požární ochraně

- vyhl. MV č. 87/2000 Sb. podmínky požární bezpečnosti při svařování
- ČSN 05 0601 Bezp. ustanovení pro sváření kovů - provoz -zvláště příkaz ke svařování na pracovištích se zvýšeným nebezpečím požáru, opatření , asistence , 8-mi hodinový následný dozor, úklid pracoviště
- ČSN 05 0610 Bezp.ustanovení pro sváření a řezání kovů plamenem –kap. 3, 4.1, 4.2, 4.5
- ČSN 05 0630 Bezp.ustanovení pro obloukové sváření kovů -kapitola 6, 7
- ČSN 06 1008 Požární bezpečnost tepelných zařízení - zejména bezpečné vzdálenosti od hořlavých předmětů, použití el. vařičů a topidel
- ČSN 65 0201 Hořlavé kapaliny, provozovny a sklady - zejména rozdělení HK do tříd, podmínky pro skladování na pracovišti (max. množství)
- ČSN 73 0802 a ČSN 73 0804 - Požární bezpečnost staveb - zejména únikové cesty
- ČSN 33 1500 Revize el. zařízení - lhůty revizí
- zákon č. 71/67 Sb. o správním řízení (správní řád)
- zákon ČNR č. 200/90 Sb. o přestupcích, ve znění pozdějších změn a doplňků
- NV 91/2010 Sb. komíny - zejména lhůty
- zákon č. 22/97 Sb. o technických požadavcích na výrobky

přednáška : 15 min.

6. Zajištění požární ochrany v době pracovního klidu nebo v době sníženého provozu

- zpřístupnění všech objektů v případě požáru (umístění náhradních klíčů)

přednáška : 10 min.

7. Rozmístění hasebních prostředků umístěných v objektu a zacházení s nimi

- proces hoření
- rozmístění a způsob použití jednotlivých druhů PHP
    - rozmistění a způsob použiti požárnich vodovodů

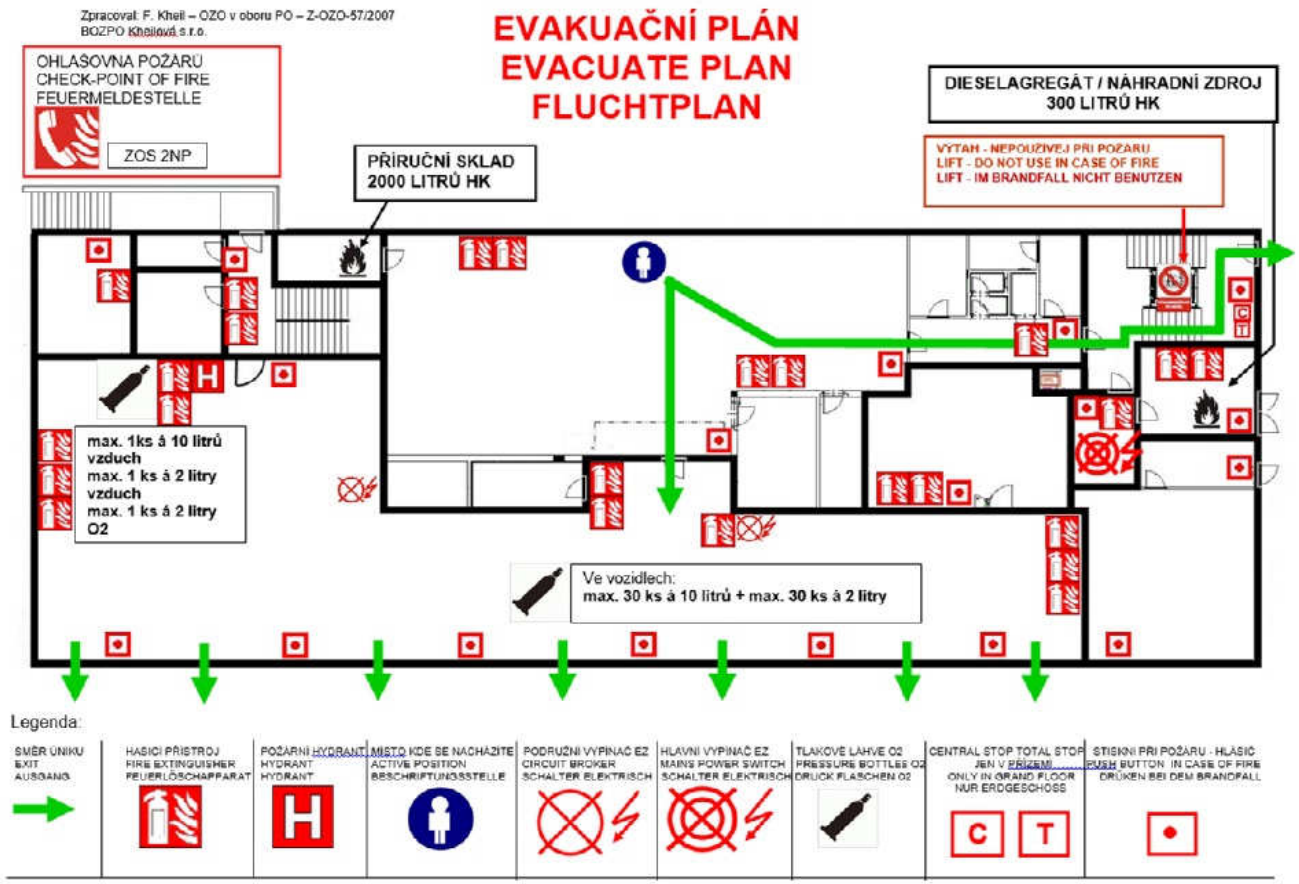
přednáška : 15 min.

Celkový časový rozsah školení : 115 min.

Příloha F **Evakuační plán 1. PP (dílny), dokumentace PO ZZS PK** – zpracovatel František Kheil OZO v oboru PO (Z-OZO-57/2007)

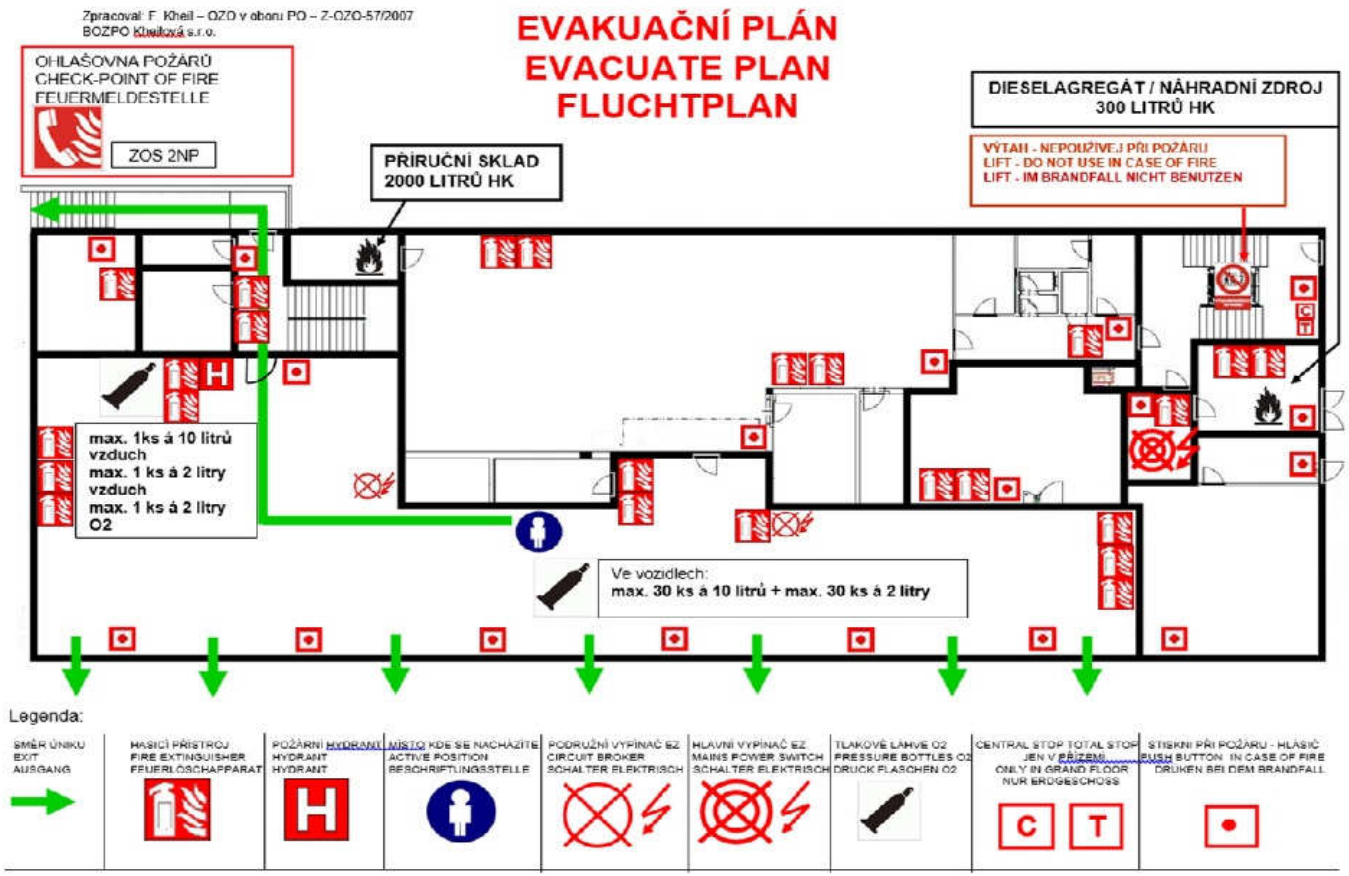
(Popis obrázku: Trasa A – od vyznačeného místa po zelené šipce směrem vpravo, Trasa B – od vyznačeného místa po zelené šipce směrem dolů)

Dílny – 3 osoby (pouze PO – PÁ, 6^{00} - 15^{30})



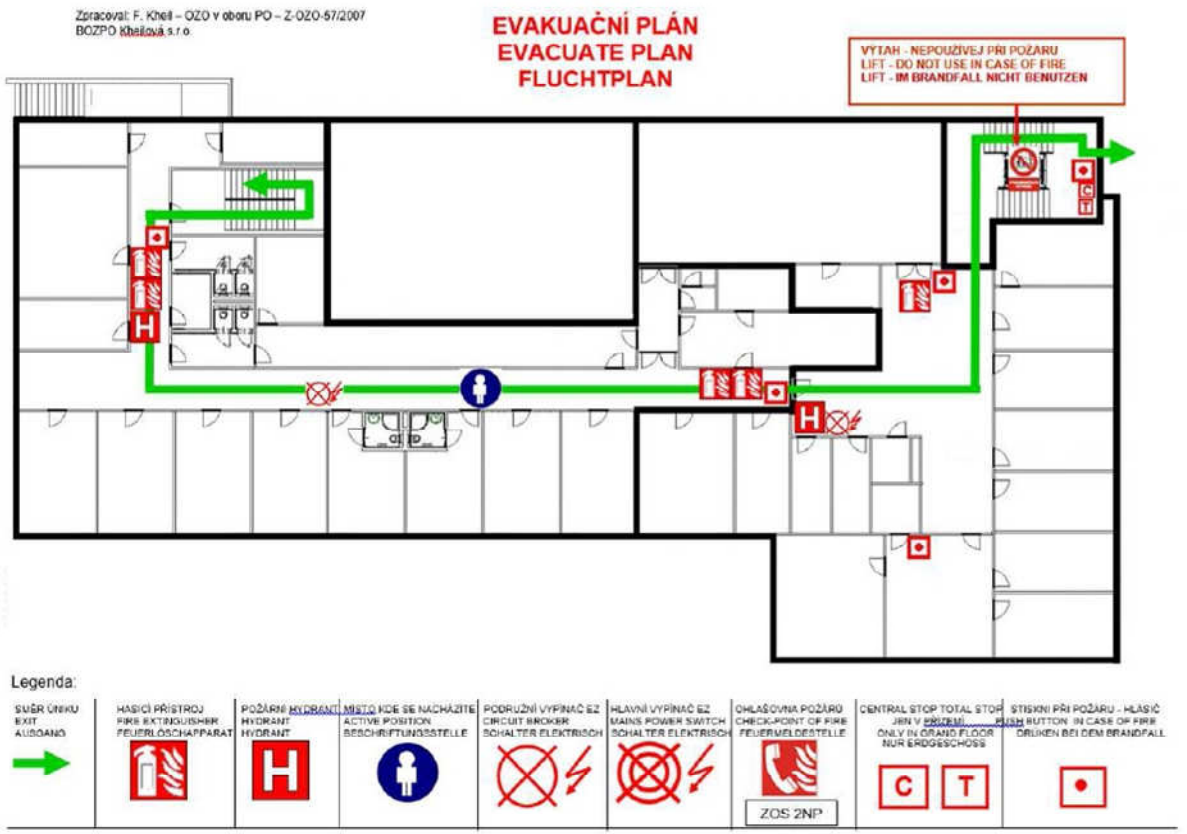
Příloha G **Evakuační plán 1. PP (garáže), dokumentace PO ZZS PK** – zpracovatel František Kheil OZO v oboru PO (Z-OZO-57/2007)

(Popis obrázku: Úniková trasa vede od vyznačeného místa po zelené šipce směrem vlevo)



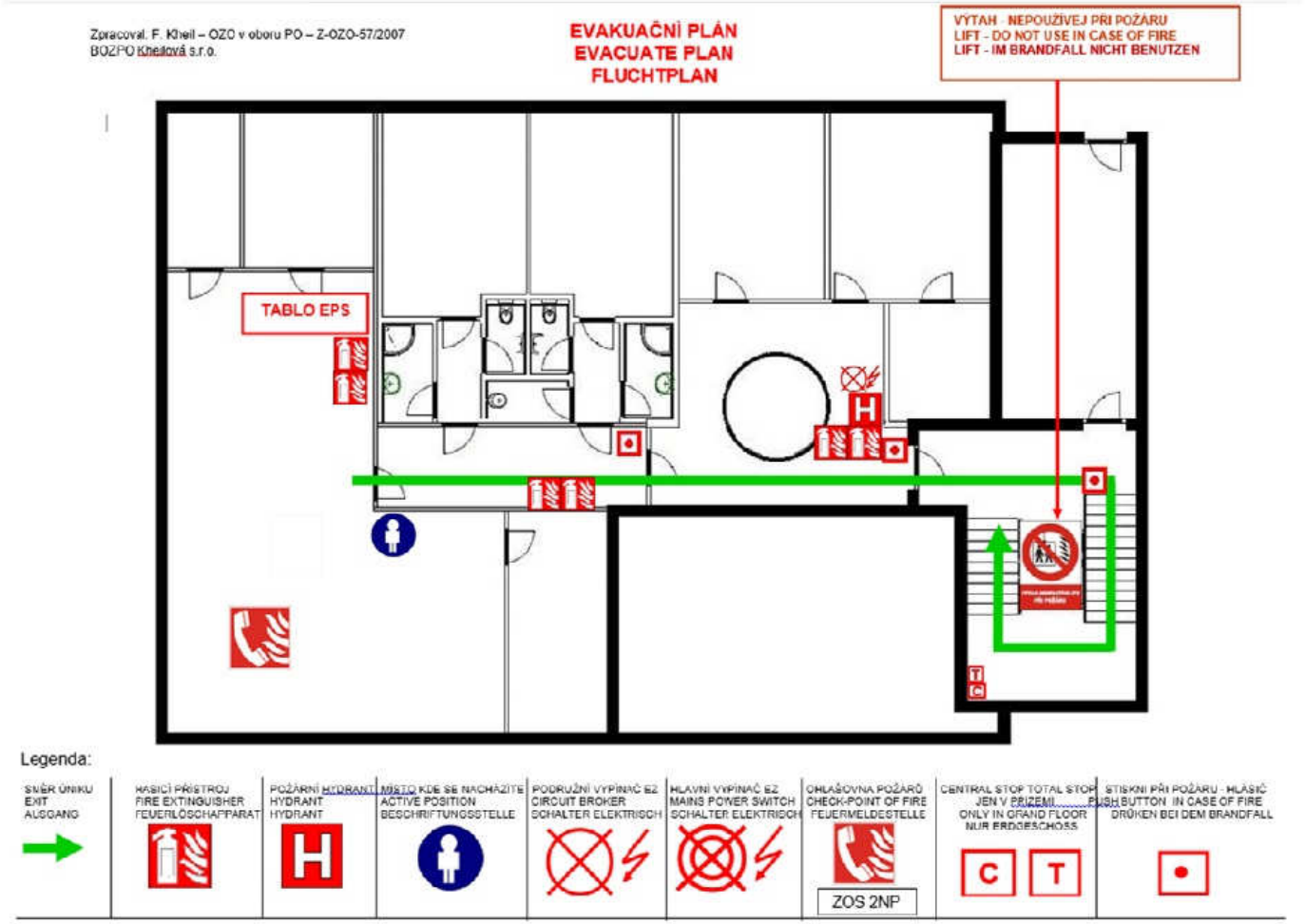
Příloha H **Evakuační plán 1.NP, dokumentace PO ZZS PK** – zpracovatel František Kheil OZO v oboru PO (Z-OZO-57/2007)

(Popis obrázku: Trasa A - od vyznačeného místa po zelené šipce směrem vpravo, Trasa B - od vyznačeného místa po zelené šipce směrem vlevo, Úniková trasa výjezdové části je totožná s Trasou A)



Příloha CH Evakuační plán 2.NP - ZOS, dokumentace PO ZZS PK – zpracovatel František Kheil OZO v oboru PO (Z-OZO-57/2007)

(Popis obrázku: Trasa vede od vyznačeného místa po zelené šipce směrem vpravo)



Příloha I Porovnání únikových tras

Místo	Počet osob	Trasa	lu	vu	E	S	Ku	U	Reálný naměřený čas (s)
1. PP (Dílny)	3	Úniková trasa A po rovině	30	35	3	1	50	3	15
		Úniková trasa A po schodech nahoru	4,7	30	3	1	30	3	
		Úniková trasa B po rovině	20,5	35	3	1	50	3	6
1. PP (2.část)		Úniková trasa po rovině	24,1	35	3	1	50	3	10
1. NP Výjezdová část	16	Úniková trasa po rovině	38,5	35	16	1	50	3	18
		Úniková trasa po schodech dolů	6,8	30	16	1	40	3	
1. NP THP trasa A	16	Úniková trasa po rovině	38,5	35	16	1	50	3	18
		Úniková trasa po schodech dolů	6,8	30	16	1	40	3	
	16 + 35	Úniková trasa po rovině	38,5	35	51	1	50	3	25
		Úniková trasa po schodech dolů	6,8	30	51	1	40	3	
1. NP THP trasa B	16	Úniková trasa po rovině	31,1	35	16	1	50	3	17
		Úniková trasa po schodech dolů	8,3	30	16	1	40	3	
	16 + 35	Úniková trasa po rovině	31,1	35	51	1	50	3	22
		Úniková trasa po schodech dolů	8,3	30	51	1	40	3	
2. NP ZOS	5	Úniková trasa po rovině	21,2	35	5	1	50	4	18
		Úniková trasa po schodech dolů	9,7	30	5	1	40	4	

K výpočtům byl použit následující vzorec:

$$t_u = \frac{0{,}75 * l_u}{v_u} + \frac{E * s}{K_u * u}$$

lu = délka únikové cesty

vu = rychlost pohybu osob v metrech

E = počet evakuovaných osob

Ku = jednotková kapacita únikového pruhu v osobách za min.

u = počet únikových pruhů (1 únikový pruh – 0,55m)

s = součinitel vyjadřující podmínky evakuace (s = 1)