

# **Návrh komplexního systému řízení ochrany a bezpečnosti objektu Nemocnice Břeclav**

Complex Security and Protection System Design  
of The Břeclav Hospital Building

Bc. Václav Mikulica

---

Diplomová práce  
2013



Univerzita Tomáše Bati ve Zlíně  
Fakulta aplikované informatiky

---

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

Jméno a příjmení: **Bc. Václav Mikulica**  
Osobní číslo: **A11376**  
Studijní program: **N3902 Inženýrská informatika**  
Studijní obor: **Bezpečnostní technologie, systémy a management**  
Forma studia: **kombinovaná**

Téma práce: **Návrh komplexního systému řízení ochrany  
a bezpečnosti objektu Nemocnice Břeclav**

### Zásady pro vypracování:

1. Provedte analýzu současného stavu z pohledu řešeného problému.
2. Vypracujte návrh řízení vybraných bezpečnostních rizik ve vybraném objektu.
3. Navrhněte vhodnou implementaci zásad pro systém řízení ochrany a bezpečnosti vybraného objektu.
4. Aplikujte zásady v rámci vybraného objektu.
5. Analyzujte aplikovatelnost vybraných zásad a jejich přínos.

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. LAUCKÝ, Vladimír. Technologie komerční bezpečnosti I. Vyd. 2. Zlín: Univerzita Tomáše Bati, 2004. 64 s. Učební texty vysokých škol. ISBN 80-7318-194-0.
2. LUKÁŠ, Luděk a kol. Bezpečnostní technologie, systémy a management I. 1. vyd. Zlín: VeRBuM, 2011. 316 s. ISBN 978-80-87500-05-7.
3. MERNA, Tony a AL-THANI, Faisal F. Risk management: řízení rizika ve firmě. Vyd. 1. Brno: Computer Press, 2007. xii, 194 s. ISBN 978-80-251-1547-3.
4. GARCIA, M. L. The design and evaluation of physical protection systems. 2nd ed. Boston: Elsevier/Butterworth-Heinemann, c2008, xviii, 351 p. ISBN 07-506-8352-X.
5. HOFREITER, L., LOVEČEK, T., VEL'AS, A., Zásady a principy analýzy rizik v oblasti fyzickej a objektovej bezpečnosti, Žilinská univerzita v Žiline, Fakulta špeciálneho inžinierstva, Žilina, 2006,.

Vedoucí diplomové práce:

**Ing. Martin Hromada, Ph.D.**

Ústav bezpečnostního inženýrství

Datum zadání diplomové práce:

**8. února 2013**

Termín odevzdání diplomové práce:

**3. června 2013**

Ve Zlíně dne 8. února 2013

  
prof. Ing. Vladimír Vašek, CSc.  
*děkan*



  
doc. RNDr. Vojtěch Křesálek, CSc.  
*ředitel ústavu*

## **ABSTRAKT**

Diplomová práce pojednává o obecných zásadách tvorby komplexního systému řízení ochrany a bezpečnosti, kde teoretická část bude následně implementována do praktického návrhu ve vztahu k objektu Nemocnice Břeclav. Práce se zabývá problematikou zabezpečení a ochrany areálu Nemocnice Břeclav.

V teoretické části je stručně popsána historie nemocnice až po její současný stav a organizační struktura. Jsou zde uvedeny základní právní rámce ochrany objektu, základní východiska bezpečnosti objektu a struktury projektu fyzické ochrany bezpečnosti.

V praktické části jsou vytyčena rizika areálu nemocnice, popsány vnitřní a vnější rizika a tyto jsou zahrnuty do následného vyhodnocení. V diplomové práci je proveden návrh zabezpečení areálu a pro zjištěná rizika jsou navrženy postupy pro jejich odstranění nebo minimalizaci.

Klíčová slova: Nemocnice, objekt, zabezpečení, riziko, ochrana

## **ABSTRACT**

This diploma thesis discusses the general principles of a comprehensive system of protection and security, where the theoretical part will be subsequently implemented in a practical proposal in relation to the object Břeclav Hospital. The thesis deals with the security and protection of the area Břeclav Hospital.

In the theoretical section briefly describes the history of the hospital to its current state and organizational structure. There are the basic legal framework for the protection object, the basic starting safety building and project structure of physical security protection.

In the practical part are risk delineated area of the hospital, described the internal and external risk and these are included in the subsequent evaluation. In this thesis the design of a security complex and the identified risk procedures are designed to eliminate or minimize them.

Keywords: Hospital, object, security, risk, protection

Děkuji Ing. Martinovi Hromadovi, Ph.D. za metodickou pomoc a rady, které mi poskytl při zpracování diplomové práce.

**Prohlašuji, že**

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

**Prohlašuji,**

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

Ve Zlíně

.....  
podpis diplomanta

**OBSAH**

<b>ÚVOD</b> .....	<b>8</b>
<b>I TEORETICKÁ ČÁST</b> .....	<b>9</b>
<b>1 DŮLEŽITÉ POJMY BEZPEČNOSTI</b> .....	<b>10</b>
1.1 REŽIMOVÁ OPATŘENÍ .....	14
1.2 FYZICKÁ OCHRANA .....	15
1.3 TECHNICKÁ OCHRANA.....	15
1.4 SYSTÉM FYZICKÉ BEZPEČNOSTI .....	16
1.4.1 Perimetrická ochrana.....	17
1.4.2 Plášťová ochrana .....	17
1.4.3 Prostorová ochrana.....	18
1.4.4 Předmětová ochrana .....	18
<b>2 PRÁVNÍ PŘEDPISY</b> .....	<b>20</b>
2.1 OSTATNÍ LEGISLATIVA.....	22
<b>3 ANALÝZA RIZIK V OBJEKTOVÉ BEZPEČNOSTI</b> .....	<b>26</b>
<b>II PRAKTICKÁ ČÁST</b> .....	<b>30</b>
<b>4 NEMOCNICE BŘECLAV</b> .....	<b>31</b>
4.1 HISTORIE NEMOCNICE.....	32
4.2 SOUČASNÁ NEMOCNICE.....	32
<b>5 BEZPEČNOSTNÍ ANALÝZA</b> .....	<b>36</b>
5.1 ZABEZPEČENÍ OBJEKTU .....	43
5.2 VÝKON OSTRAHY OBJEKTU .....	44
5.3 ELEKTRONICKÉ SYSTÉMY .....	49
5.4 KAMEROVÉ SYSTÉMY .....	54
5.5 PROTIPOŽÁRNÍ OPATŘENÍ .....	57
5.6 PŘEHLED A HODNOCENÍ MOŽNÝCH RIZIK.....	57
<b>6 NÁVRH KOMPLEXNÍHO SYSTÉMU OCHRANY A BEZPEČNOSTI</b> .....	<b>63</b>
6.1 NÁVRH OPATŘENÍ KE SNÍŽENÍ ZJIŠTĚNÝCH RIZIK .....	64
<b>ZÁVĚR</b> .....	<b>69</b>
<b>CONCLUSION</b> .....	<b>71</b>
<b>SEZNAM POUŽITÉ LITERATURY</b> .....	<b>73</b>
<b>SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK</b> .....	<b>76</b>
<b>SEZNAM OBRÁZKŮ</b> .....	<b>78</b>
<b>SEZNAM TABULEK</b> .....	<b>79</b>
<b>SEZNAM PŘÍLOH</b> .....	<b>80</b>

## ÚVOD

V diplomové práci chci zjistit dosavadní zabezpečení areálu Nemocnice Břeclav, příspěvkové organizace (dále jen Nemocnice Břeclav: nemocnice) jak po stránce fyzické bezpečnosti, tak po stránce zákonných předpisů a legislativních předpisů obecně. Na základě zjištěných informací vytyčím možná rizika a navrhnu komplexní systém řízení ochrany a bezpečnosti objektu Nemocnice Břeclav pro minimalizaci případných nebezpečí nebo jejich úplnou eliminaci.

Nemocnice jsou důležité objekty poskytující zdravotnickou a ošetrovatelskou péči pro širokou veřejnost. Tato informace naznačuje, že v takových objektech se shromažďují velké počty lidí vyhledávajících ambulantní péči případně hospitalizaci a to jsou aspekty podmiňující pro velkou ostražitost nad bezpečnostními opatřeními a provozními řády v takových objektech. Nemocnice jsou veřejné budovy jejichž hlavním cílem je poskytování kvalitní zdravotní péče tedy předpokládá se četný pohyb osob potažmo pacientů. Takto jsou vnímána zdravotnická zařízení širokou veřejností, ale jen málokdo se pozastaví nad tím, jak bezpečné je vše v jejím nitru. Bezpečnost je vnímána jako jedna ze základních potřeb člověka dle Maslowovy pyramidy potřeb, což potvrzuje důležitost vnímání tohoto kritéria pro člověka.

Diplomová práce může být vodítkem pro vedení jiných nemocnic podobného typu, jak přehodnotit stávající zabezpečení daného objektu, osob a dokumentace jež se nachází uvnitř.

První část diplomové práce je zaměřena na teoretický výklad pojmů a definic jako je bezpečnost, kontrola a bezpečnostní řešení. Druhá část obsahuje popis nemocnice a praktickou část, kdy je popsán stávající stav zabezpečení a ochrany s následným návrhem komplexního řešení řízení ochrany objektu.

Cílem diplomové práce je zjistit a popsat aktuální stav zabezpečení areálu nemocnice a určit rizika bezpečnosti v návaznosti na to navrhnout komplexní systém řízení ochrany a bezpečnosti objektu nemocnice.

Zdrojem informací diplomové práce byla především knižní literatura, články dostupné na internetu, informace získané z interní řízené dokumentace, aktuálních právních předpisů a profesní zkušenosti vedoucího diplomové práce.



## **I. TEORETICKÁ ČÁST**

## 1 DŮLEŽITÉ POJMY BEZPEČNOSTI

Bezpečnost subjektu je chápána jako stav, kde rizika plynoucí z hrozeb jsou eliminována na akceptovatelnou úroveň. Má-li se subjektu zajistit bezpečnost, musí být známy základní hrozby, které mu mohou způsobit újmu. Mezi základní hrozby v současnosti patří činnost kriminálních živlů případně jiných osob, jejichž cílem je zcizení, neoprávněné nakládání, poškození nebo úplné zničení chráněných aktiv [2].

Způsob provedení či naplnění hrozby určuje opatření, jimiž se zajišťuje ochrana proti jejich účinku. Ochrana v obecném pojetí představuje vytvoření bezpečného prostředí pro daný subjekt. Realizace ochrany představuje návrh a sladění všech dostupných prostředků, které zajistí požadovanou nebo definovanou bezpečnost. Bezpečnostní opatření, realizovaná ve formě systému fyzické bezpečnosti, jsou schopna potencionálního narušitele odradit od jeho činu, zamezit jeho provedení, případně jej zpomalit při zcizení aktiv. Soudobý systém fyzické bezpečnosti objektu (ochrany majetku) zpravidla zahrnuje režimová opatření, fyzickou ochranu a technickou ochranu (technické prostředky fyzické bezpečnosti).

Bezpečnostní politika firmy či organizace je důležitým bodem strategického plánu a neodmyslitelnou součástí v rozhodování managementu. Bezpečnostní politika je dokument mající charakter všeobecného plánu v oblasti bezpečnosti. Bezpečnostní politika určuje rámec bezpečnosti organizace a je po schválení vedením organizace závazná pro všechny její zaměstnance. Musí být v souladu s politikou celé organizace, definuje základní strategii, postoje, role, cíle a zásady týkající se činností spojených s bezpečností. Vychází z existujících a platných interních směrnic a politik, jež rozvíjí prostředí organizace. Akceptuje závěry z analýz rizik v organizaci a definuje postupy zajišťující efektivnější řízení bezpečnosti.

Rostoucí agresivita osob ošetřovaných nebo dožadujících se ošetření na ambulancích nemocnic, mnozí se krádeže majetku pacientů, personálu i organizací jsou impulsem pro vytvoření komplexního systému bezpečnosti ve zdravotnických zařízeních s nepřetržitým provozem.

Hrozba je jakýkoli fenomén, který má potenciální schopnost poškodit zájmy a chráněné hodnoty. Zranitelné místo je takové místo, kde může vzniknout následné riziko nebezpečí. Útočník je osoba ohrožující napadající osobu nebo skupinu osob, ohrožující majetek a jiné hodnoty.

Kontrolní činnost je důležitým prvkem fungujícího bezpečnostního systému ochrany. Pokud nebudeme respektovat zásady kontrolní činnosti, nemůžeme se ucházet o dosažení systému jakosti, nemůže dojít k žádnému zkvalitnění naší činnosti. Kontrolou rozumíme kritické zhodnocení reality (skutečného stavu) v porovnání se záměry, úkoly, plánem, projektem, standardy apod. Kontrola v technických systémech nebo v direktivním řízení představuje zpětnou vazbu, pomocí níž se získává objektivní představa o řízené realitě. V minulosti se využívala zejména kontrola na výstupu. Dnes se provádí tzv. průběžná kontrola v rámci procesů a předběžná kontrola. Kontrolní činnosti mohou být vnitřní a vnější. Do zásad kontrolní činnosti patří pravidelnost, cílevědomost, odbornost, objektivnost, konkrétnost, optimálnost a efektivnost.

Zásada pravidelnosti říká, že pokud nebude kontrola stálá, nepřetržitá, musí být alespoň pravidelná v určitých pravidelných etapách tak, aby zaručovala výsledky a nutila kontrolované útvary pracovat kvalitně, jakostně, neustále a pouze kvalitu doladovat [1].

Zásada cílevědomosti říká, že každou kontrolu neděláme pouze pro kontrolu, ale s nějakým cílem a tím cílem je především jakost dosahování jakostního (kvalitního) produktu [1].

Zásada odbornosti spočívá v tom, že kontrolní činnosti musí provádět specialista odborník, který danou činnost perfektně ovládá a má na ni potřebnou certifikaci, odbornost a vzdělání [1].

Zásada objektivnosti praví, že každá kontrolní činnost musí být provedena vždy objektivně, tj. věcně, předmětně, spravedlivě a nestranně. Bez emocí a záští [1].

Zásada konkrétnosti znamená, že proces kontroly se zakládá vždy na hodnověrných informacích z procesu řízení, které jsou získány na vědeckých zásadách. Kontroluje se konkrétní jev, skutek, počín, dílo, činnost. Kontrolní činnost nelze konat na základě „keců“ a různých blamáží, v zásadě neprověřené informace nelze brát jako výchozí základ kontroly [1].

Zásada optimálnosti a efektivnosti znamená rychlost, jednoduchost, spojení úkolů za podmínky využití minimálních sil a prostředků. Nebudeme řešit kontrolní činnost, kterou lze udělat za dva dny celý měsíc kontrola musí být účelná, účinná a působivá [1].

Rozhodování je jádrem řízení a uplatňuje se v jakýchkoliv manažerských činnostech. Při manažerském rozhodování jde o kombinaci vědy a umění rozhodovat. Kvalita a výsledky rozhodovacích procesů ovlivňují zásadním způsobem efektivnost fungování a budoucí

prosperitu celých organizací. Věcná stránka rozhodování vyplývá z odlišností obsahu jednotlivých rozhodovacích procesů (výroba, vývoj, investice, organizační struktura, spolupráce mezi firmami, výběr pracovníků). Věcnou stránku pomáhají řešit specialisté daného oboru. Formálně logická stránka rozhodování představuje to, co jednotlivé rozhodovací procesy spojuje, co představuje proceduru řešení. Ty jsou obsahem teorie rozhodování. Objektem teorie rozhodování jsou rozhodovací procesy a rozhodovací problémy.

**Rozhodovacím procesem** rozumíme proces řešení rozhodovacího problému. Základním charakteristickým znakem rozhodování je možnost volby, tj. posuzování jednotlivých variant a výběr rozhodnutí (optimální varianta, výběr reálných variant řešení)

**Rozhodovací problém** znamená rozdíl (diferenci) mezi žádoucím stavem a jejím skutečným stavem. Například rozdíl mezi předpokládaným a skutečným objemem zakázek, rozdíl mezi projektovanými a skutečnými náklady, rozdíl mezi evidenčním a skutečným stavem pracovníků atp. Tyto problémy byly zjištěny jako reálné problémy.

Určité problémy však mohou vznikat až v budoucnu. Jde o potenciální problémy a ty mohou firmu ohrožovat nebo pro ni vytvářet podnikatelské příležitosti. Může jít např. o změny zákonů, nebo růst či pokles kriminality ve společnosti, vstup konkurenčních firem na trh, růst cen pohonných hmot, zásadní změny technologie apod. Vlastní rozhodnutí představuje výběr varianty určené k realizaci. Kvalitu rozhodování ovlivňuje řada faktorů. Patří mezi ně racionální postupy řešení rozhodovacích problémů a používané metody a modely rozhodování.

**Riziko** je v komplexním pojetí chápáno jako relace mezi očekávanou ztrátou (poškození zdraví, ztrátou života, ztrátou majetku apod.) a neurčitostí uvažované ztráty (většinou vyjádřena pravděpodobností nebo frekvencí výskytu).

**Analýza rizik** je systematické používání informací k odhadu rizika a k identifikaci jeho zdrojů.

**Vyhodnocení rizik** je proces porovnávání odhadnutého rizika vůči daným kritériím pro určení jeho významu.

**Management rizik** jsou koordinované činnosti sloužící k řízení a kontrole organizace s ohledem na rizika.

**Nežádoucí událost** je událost nebo okolnost, která může vyústit nebo vyústila v tělesné poškození pacienta, kterému bylo možné se vyhnout. Dále jsou za nežádoucí události považovány případy, kdy poškození pacienta je pouze psychické či socioekonomické a také případy, kdy poškozeným je zdravotnické zařízení nebo jeho pracovník.

**Preventivní opatření** jsou opatření k odstranění příčiny potenciální neshody nebo jiné potenciální nežádoucí situace. Může existovat více než jedna příčina potenciální neshody. Preventivní opatření se přijímá s cílem zabránit výskytu, zatímco nápravné opatření se přijímá s cílem zabránit opětovnému výskytu.

Povinností odpovědného vedoucího zaměstnance popřípadě pracovníka BOZP je kontrolovat, že stanovená i existující opatření jsou realizována a to zejména u možných následků ohrožení.

Při stanovení postupů a opatření ke snížení a zvládnutí rizik a jejich priorit platí následující zásady:

- odstranění zdroje rizika
- minimalizace zdroje rizika
- úplná separace zdroje rizika
- částečné krytí zdroje rizika
- oddálení člověka z pole zdroje rizika úrazu, nebezpečného prostoru
- snížení pravděpodobnosti působení zdroje rizika
- zvýraznění zdroje rizik (bezpečnostní sdělení apod.)

V otázce komplexní bezpečnosti je nutno brát na zřetel i ochranu dat a informací nacházejících se v objektu nemocnice. V této diplomové práci se chci zaměřit na fyzickou a technickou ochranu zabezpečení, proto uvedu k informačním technologiím pouze pár důležitých pojmů.

**Dostupnost** je zajištění, že informace je pro oprávněné uživatele přístupná v okamžiku její potřeby.

**Důvěrnost** je zajištění, že informace jsou přístupné nebo sděleny pouze těm, kteří jsou k tomu oprávněni.

**Bezpečnost informací** je zachování důvěrnosti, integrity a dostupnosti informací a dalších vlastností jako jsou autentičnost, odpovědnost, nepopiratelnost a spolehlivost.

**Osobní údaj** je jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.

Nemocniční informační systém je interní program zajišťující komunikaci a shromažďování lékařských a osobních dat. Jeho popis, provoz a zabezpečení v rámci tohoto zdravotnického zařízení je popsán v diplomové práci Bc. Petra Baťky, vedoucího oddělení nemocniční informatiky a telekomunikací v Nemocnici Břeclav, příspěvkové organizaci.

**Fyzickou bezpečnost** tvoří systém opatření, která mají neoprávněným osobám zabránit nebo ztížit přístup do chráněného objektu. Soudobý systém fyzické bezpečnosti objektu (ochrany majetku) zpravidla zahrnuje:

- režimová opatření
- fyzickou ochranu (činnost fyzické ostrahy)
- technickou ochranu (technické prostředky systému fyzické bezpečnosti)

## 1.1 Režimová opatření

Režimová opatření představují procesní naplnění bezpečnostní politiky organizace. Cílem režimových opatření je stanovit zásady, pravidla, oprávnění při pohybu zaměstnanců a dalších osob v prostorách organizace, způsob nakládání s bezpečnostně důležitými prvky, pravidla provádění bezpečnostních kontrol vnášeného a vynášeného materiálu apod.

Režimová opatření by měla být navržena tak, aby příliš neomezovala pohyb osob v objektu organizace a současně zajistila požadovaný stupeň bezpečnosti. Významnou roli v této oblasti sehrává systém kontroly vstupu.

Povinnosti subjektu k zavedení režimových opatření mohou vyplývat z právních předpisů upravujících jeho činnost nebo z podmínek pro její výkon. Režimová ochrana je v rámci systému fyzické ochrany pojítkem zbylých částí tedy technické ochrany a fyzické ochrany. Základem pro režimovou ochranu podobně jako pro celý systém fyzické ochrany jsou dokumenty Bezpečnostní politika a analýza bezpečnostních rizik [2].

## 1.2 Fyzická ochrana

Bezpečnostní situace zahrnují v rámci zajištění fyzické bezpečnosti široké spektrum událostí. Adekvátní reakce vyžadují určené a hlavně speciálně připravené osoby, schopné zajistit bezpečnost chráněných aktiv adekvátní a efektivní cestou s minimálními dopady. Fyzická ostraha, zajišťující fyzickou ostrahu střeženého objektu, plní v této oblasti významnou roli. Svoji trvalou či dočasnou přítomností v objektu organizace je schopna v souladu s režimovými opatřeními zajistit ochranu aktiv. Jedná se především o odhalení a zadržení narušitele, zamezení zcizení aktiv, realizaci protipožárních a havarijních opatření apod. Fyzická ochrana bývá prováděna strážnými, hlídači, hlídací službou či policisty. Většina organizací zajišťuje svoji fyzickou ochranu jako službu poskytovanou jiným právním subjektem, zpravidla soukromou bezpečnostní službou. Zajišťování fyzické ochrany ostrahou bývá zpravidla finančně nejnákladnější způsob zajištění bezpečnosti [2].

## 1.3 Technická ochrana

Technické prostředky fyzické bezpečnosti současně s fyzickou ostrahou představují základní bezpečnostní opatření fyzické bezpečnosti objektu. Cílem technických prostředků je podpořit realizaci režimových opatření, zkvalitnit činnost fyzické ostrahy a odradit narušitele od jeho činu, případně významně ztížit činnost a prodloužit dobu jeho přístupu k chráněným aktivům. Mezi základní technické prostředky fyzické bezpečnosti se řadí mechanické zábranné systémy a elektronické bezpečnostní systémy. Mechanické zábranné systémy zahrnují dveře, zámky, ploty, mříže ostnaté dráty apod., které svými vlastnostmi brání fyzickému pohybu narušitele. Cílem elektronických bezpečnostních systémů je řízení přístupu k aktivům organizace a odhalení neoprávněného přístupu k nim. Mezi základní

elektronické bezpečnostní systémy řadíme systémy kontroly vstupu, elektronickou požární signalizaci, kamerové systémy a poplachové zabezpečovací systémy.

Všechny zabezpečovací systémy a jejich požadavky jsou podrobně popsány v technických normách tvořených a vydaných Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví. Požadavky na technické parametry a odolnost komponentů požárních a poplachových systémů, elektromagnetickou kompatibilitu a metody zkoušek vlivu prostředí řeší normy z řady ČSN EN 50 130 Poplachové systémy.

Poplachový zabezpečovací systém je ve své podstatě digitální elektronický systém, který ve střeženém prostoru trvale monitoruje specifické fyzikální projevy a při jejich výskytu vyhláší poplach. Specifickými fyzikálními projevy jsou demaskující projevy přítomnosti narušitele ve střeženém prostoru, spojené zejména s jeho pohybem. Jedná se například o změnu kmitočtu akustických vln, odražených od povrchu těla narušitele, vyzařováním infračerveného záření tělem narušitele, přerušeni paprsku infračerveného záření tělem narušitele, sepnutí spínače pohybem apod. Poplachové zabezpečovací systémy jsou zpravidla složeny z ústředny, optických a akustických výstražných prvků, detektorů narušení a přímých spojů, zajišťujících připojení detektorů do ústředny. Ústředna zajišťuje příjem poplachů z jednotlivých detektorů narušení, jejich zaznamenání, vyhodnocení a vyhlášení poplachu. Ústředna poplachového zabezpečovacího systému může být připojena prostřednictvím poplachového přenosového systému na poplachové příjímá centrum (pult centralizované ochrany). Detektory narušení tvoří senzorickou část poplachového zabezpečovacího systému [2].

#### **1.4 Systém fyzické bezpečnosti**

Mezi výsledky optimalizace bezpečnostního systému objektu patří vymezení principů, uplatněných při jeho návrhu a realizaci. Jedním z těchto principů je princip vícestupňovosti ochrany. Podstata tohoto principu spočívá ve vymezení základních stupňů při zajištění fyzické bezpečnosti, které představují určité hranice, oblasti či domény, které musí narušitel překonat při postupu v objektu k předmětu jeho zájmu.

Základními stupni ochrany jsou:

- perimetrická ochrana



- plášťová ochrana
- předmětová ochrana

Každý z výše uvedených stupňů ochrany má svá specifika, která vychází z určení, pořadí a prostorových dispozic dané ochrany. Technické prostředky, použité k jejímu zajištění, musí respektovat požadavky. Z hlediska detektorů narušení se jedná o typ monitorovaných demaskujících příznaků narušitele, tvar a dosah detekční charakteristiky, citlivost a odolnost vůči planým poplachům [2].

#### **1.4.1 Perimetrická ochrana**

Perimetrická ochrana představuje souhrn bezpečnostních opatření fyzické bezpečnosti, uplatněných na obvodu pozemku (parcely) chráněného objektu a v prostoru mezi jeho hranicí a chráněným objektem. Perimetrem je jeho katastrální hranice, která bývá vymezena přírodními nebo umělými bariérami. Cílem perimetrické ochrany je především odstrašení, odhalení a zpoždění narušitele. Perimetrická ochrana by měla signalizovat narušení obvodu objektu. Vzhledem k různorodosti vnějšího venkovního prostředí i široké škále pohybujících se objektů bývá odolnost vůči planým poplachům problematickou. V současnosti se stává perimetrická ochrana samostatnou oblastí technické ochrany [2].

#### **1.4.2 Plášťová ochrana**

Plášťová ochrana je souhrnem všech bezpečnostních opatření fyzické bezpečnosti realizovaných na plášti chráněného objektu, zpravidla budovy. Cílem plášťové ochrany je odstrašení, znemožnění průchodu, zpoždění a odhalení narušitele. Plášťová ochrana signalizuje jakékoliv významné narušení pláště budovy. Plášťovou ochranu tvoří stěny, okna, dveře, zámky a zámkové systémy, mříže, bezpečnostní fólie, kamerové systémy, detektory narušení atd. Detekční prvky plášťové ochrany se zpravidla umísťují zevnitř budovy. Detektory narušení mají plochou, ale širší detekční charakteristiku a kratší dosah. Pokud jsou detektory narušení umístěny vně budovy, musí rovněž splňovat požadavky na vyšší klimatickou odolnost [2].

### 1.4.3 Prostorová ochrana

Cílem prostorové ochrany je zpoždění a odhalení pohybu narušitele uvnitř střežené budovy. Opatření prostorové ochrany jsou realizována ve vnitřních prostorech budovy, zpravidla na chodbách, schodištích a v místnostech. Prostorovou ochranu tvoří dveře, mříže, zámky a zámkové systémy, kamerové systémy, systémy kontroly vstupu a poplachové zabezpečovací systémy s detektory narušení. Detektory narušení by měly v rámci prostorové ochrany signalizovat vniknutí do vnitřních prostor budovy. Použité detektory narušení mají většinou kratší dosah a širší kuželovou detekční charakteristiku. Klimatická odolnost takového detektoru musí vždy odpovídat požadavkům pro vnitřní prostředí. V případě zdravotnického zařízení musí také splňovat interní požadavky daných oddělení v návaznosti na hygienické požadavky takového prostředí [2].

### 1.4.4 Předmětová ochrana

Předmětovou ochranu tvoří opatření vedoucí k zamezení zcizení a neoprávněné manipulaci s chráněnými aktivy. Chráněnými aktivy jsou obvykle cenné předměty, patentově chráněné vzory a další, z jakéhokoliv důvodu cenné fyzické předměty. Předmětovou ochranu tvoří vitríny, skleněné tabule, kamerové systémy a poplachové zabezpečovací systémy. Detektory narušení by měly identifikovat bezprostřední přítomnost narušitele u chráněného předmětu nebo jakoukoliv manipulaci s ním. Detektory narušení, předurčené k monitorování přítomnosti narušitele, mají obvykle širokoúhlou a plochou detekční charakteristiku s krátkým dosahem [2].

Úroveň jednotlivých ochranných opatření by měla vždy odpovídat hodnotě chráněných aktiv a stupni zabezpečení. Je neefektivní vynakládat na bezpečnostní opatření náklady, které převyšují samotnou hodnotu chráněných aktiv [2].

**Ochrana objektu** je charakterizována odolností prvků ochrany na cestě pachatele a schopností eliminovat jeho činnost v určitém bodu.

Vzhledem k tomu, že prioritou je ochrana zdraví a životů lidí nacházejících se v objektu nemocnice musí být brán na zřetel význam vložených prostředků do ochrany bezpečnosti takových osob nejen po dobu ambulantní návštěvy zařízení, ale hlavně s ohledem na hospitalizované pacienty a samozřejmě na zaměstnance organizace. Důležitým parametrem

je i ochrana majetku a objektu jako celku aby nedošlo k jakémukoliv narušení bezpečnosti a tím ohrožení provozu zdravotnického zařízení.

V nemocnici jakožto zdravotnické zařízení pro poskytování zdravotnické péče v nepřetržitém provozu, je nutno brát na zřetel také možnost napadení objektu a personálu zajišťujícím léčebně preventivní péči nebo zdravotnickou a následnou péči. Stejně tak může dojít k napadení ostrahy objektu a tím ochromení zajištění ochrany objektu a osob v něm nacházejících.

**Napadnutí objektu** je činnost pachatele vykonávaná od hranice zajmového prostoru až po dosáhnutí svého cíle a následného úniku.

**Bezpečnostní odolnost objektu** je možno chápat jako vlastnost objektu vyznačující se schopností odolávat úsilí pachatele dosáhnout svého cíle.

## 2 PRÁVNÍ PŘEDPISY

Jedním ze základních právních předpisů zajišťujících právo na život a jeho ochranu je Listina základních práv a svobod, která je součástí ústavního pořádku České republiky. Základní práva a svobody obsažené v Listině v zásadě stanovují vztah mezi státem a občanem České republiky. Listina základních práv a svobod vychází z principů právního státu to je ze svrchovanosti práva a zásady možnosti zásahu moci státní do svobod jednotlivce pouze na základě a v mezích platného zákona. V České republice vstoupila v platnost 28. prosince 1992.

Trestní řád dává oprávnění kterékoli osobě (kdokoli) omezit osobní svobodu osoby, která byla přistižena při trestním činu nebo bezprostředně poté, tedy toto oprávnění má i bezpečnostní pracovník. Ten, kdo takovou osobu omezil na osobní svobodě je však povinen ihned ji odevzdat policejnímu orgánu, příslušníku ozbrojených sil, vojenské policii nebo nejbližšímu vojenskému útvaru, nebo nemůže-li takovou osobu odevzdat, je povinen tyto orgány o omezení ihned informovat [1].

Zákon č. 372/2011 Sb. upravuje zdravotní služby a podmínky jejich poskytování a s tím spojený výkon státní správy, druhy a formy zdravotní péče, práva a povinnosti pacientů a osob pacientům blízkých, poskytovatelů zdravotních služeb, zdravotnických pracovníků, jiných odborných pracovníků a dalších osob v souvislosti s poskytováním zdravotních služeb, podmínky hodnocení kvality a bezpečí zdravotnických služeb, dalších činností související s poskytováním zdravotních služeb a zpracovává příslušné předpisy Evropské unie. Dle zákona č. 372/2011 Sb., o zdravotních službách, nemocnice zajišťuje poskytování zdravotních služeb v případech hromadného neštěstí, v návaznosti na traumatologický plán havarijního plánu Jihomoravského kraje.

Nemocnice v souladu se zřizovací listinou, platnou legislativou, zejména zákonem č. 372/2011 Sb., o zdravotních službách, ve znění pozdějších předpisů, a vnitřními předpisy, zpracovává osobní a citlivé údaje pacientů pro účely poskytování zdravotní péče a další informace související s činností zdravotnického zařízení. Veškeré informace týkající se pacientů v jakékoliv formě jsou v nemocnici považovány za důvěrné a musí s nimi jako s důvěrnými být nakládáno. Použití těchto informací při dalším zpracování je omezeno a jsou zpracovány v rozsahu nezbytně nutném pro zajištění požadovaného či stanoveného

výstupu nebo činnosti. V těch částech kde to jde jsou informace zpracovány formou anonymního údaje.

Zákon č. 101/2000 Sb., o ochraně osobních údajů v souladu s právem Evropských společenství, mezinárodními smlouvami, kterými je Česká republika vázána, a k naplnění práva každého na ochranu před neoprávněným zasahováním do soukromí upravuje práva a povinnosti při zpracování osobních údajů a stanovuje podmínky, za nichž se uskutečňuje předání osobních údajů do jiných států.

Zákoník práce §31b v tomto ustanovení dává kterémukoliv zaměstnavateli oprávnění, aby k ochraně svého majetku prováděl v nezbytném rozsahu kontrolu věcí, které zaměstnanci vnášejí nebo vynášejí z organizace, popř. prováděl prohlídky zaměstnanců. Při kontrole a prohlídce musí být dodrženy právní předpisy o ochraně osobní svobody a nesmí být ponižována lidská důstojnost. Prohlídku může provádět jen osoba stejného pohlaví. Jestliže si nás zaměstnavatel za úplatu najímá jako službu, abychom za něho tuto kontrolní činnost prováděli, pak na nás také přenáší (deleguje) oprávnění, které mu dává zákoník práce [1].

Zákonem č. 40/2009 Sb., trestní zákoník ve znění pozdějších změn byla provedena rektifikace trestního práva hmotného. Došlo ke změně přístupu k trestněprávní ochraně významných společenských zájmů. Preferují se základní lidská práva a svobody nad ostatními zájmy. K hlavním změnám patří ustanovení o trestním činu, kde se uvádí “trestním činem je protiprávní čin, který trestní zákon označuje za trestný a který vykazuje znaky uvedené v takovém zákoně” Tímto došlo ke zrušení posuzování společenské nebezpečnosti. Dle §14 se trestné činy dělí na přečiny a zločiny, přičemž přečiny jsou všechny nedbalostní trestné činy a ty úmyslné trestné činy jsou trestné činy s horní hranicí trestní sazby do pěti let. Podle §20 je příprava trestná pouze pokud je tak u příslušného trestného činu výslovně uvedeno [12]. Trestní zákoník popisuje všechny důležité pojmy v souvislosti s ochranou osob a majetku. Nutná obrana je zde popsána jako „ Čin jinak trestný, kterým někdo odvrací přímo hrozící nebo trvajícím útok na zájem chráněný trestním zákonem, není trestným činem. Nejde o nutnou obranu, byla-li obrana zcela zjevně nepřiměřená způsobu útoku.“ Podstatou nutné obrany je odvrácení útoku na zájem chráněný trestním zákonem a to činem, který by byl jinak trestným činem namířeným proti útočníkovi. Protože však ten, kdo útok odvrací, chrání tytéž zájmy, které chrání trestní zákon sám, nejedná proti účelu trestního zákona, ale ve shodě s ním. Jeho čin nahrazuje vlastně zásah veřejných orgánů. K nutné obraně je oprávněn kdokoliv, nejen ten, kdo byl

sám bezprostředně ohrožen. Je-li útočníků více, může obrana směřovat proti kterémukoliv z nich [1]. Krajní nouze je definována jako čin jinak trestný, kterým někdo odvrací nebezpečí přímo hrozící zájmu chráněnému trestním zákonem, není trestním činem. Nejde o krajní nouzi, jestliže bylo možno toto nebezpečí za daných okolností odvrátit jinak anebo způsobený následek je zřejmě stejně závažný nebo ještě závažnější než ten, který hrozil. Podstatou krajní nouze je odvrácení nebezpečí přímo hrozícího zájmům chráněným trestním zákonem a to činem, který by byl jinak trestným činem. Dochází zde ke střetu dvou chráněných zájmů, kdy na záchranu ohroženého zájmu je nutno obětovat zájem jiný, méně závažný [1].

## 2.1 Ostatní legislativa

Organizace, které jsou držitelem mezinárodních certifikátů ISO jsou vázány na plnění daných mezinárodních norem.

Norma ISO 9001 stanovuje zásady, kdy vedení firmy stanoví své cíle a plány v oblasti kvality a tyto jsou postupně pomocí nastavených procesů realizovány, přičemž účinnost těchto procesů je pravidelně měřena a monitorována, aby společnost mohla přijmout účinná opatření na změnu. Norma se zabývá principy řízení dokumentace, lidských zdrojů, infrastruktury, zavádí procesy komunikace se zákazníky, hodnocení dodavatelů, měření výkonnosti procesů a interní audity pro účely zpětné vazby.

Norma OHSAS 18 001 stanovuje zásady, kdy vedení firmy stanoví své cíle a plány v oblasti snižování pracovních úrazů a nehod a tyto jsou postupně pomocí nastavených procesů realizovány. Přináší systematické omezování rizik a nebezpečí, která ohrožují bezpečnost a zdraví všech zaměstnanců, přináší účinný systém reagující pružně na změny požadavků z legislativních předpisů, bezpečnostních požadavků i změn uvnitř organizace. Společně s normami ISO 9001 a ISO 14 001 tvoří integrovaný manažerský systém.

Norma ČSN CLC/TS 50131-7 obsahuje pokyny pro aplikace poskytující návod pro navrhování, montáž, provoz a údržbu poplachových zabezpečovacích a tísňových systémů (Intruder and Hold-up Alarm Systems – v překladu PZTS). Účelem tohoto dokumentu je zajistit, aby systémy PZTS splňovaly požadované funkční vlastnosti při minimálním množství planých poplachů. Tyto pokyny pro aplikace jsou sestaveny v logickém pořadí, v němž obvykle návrh a montáž systémů PZTS probíhá. Každý krok je popsán samostatně,

ale předpokládá se, že v praxi mohou být některé kroky prováděny současně. Příloha K popisuje formou vývojového diagramu hlavní procesy a dokumentaci obsaženou v tomto aplikačním návodu. Osoby odpovědné za návrh, přípravu montáže, montáž, předání, provoz a údržbu PZTS, mají být dobře obeznámené s dalšími evropskými normami vztahujícími se k PZTS, zejména s těmi, které se týkají systémových požadavků, ovládacích a indikačních zařízení, detektorů, výstražných zařízení, napájecích zdrojů a poplachových přenosových systémů.

Tyto pokyny pro aplikace jsou rozděleny do sedmi hlavních kapitol; jejich stručné vysvětlení je uvedeno v následujících odstavcích:

- **Kapitola 7 – Návrh systému**

Tato kapitola je určena jako vodítko pro osoby odpovědné za návrh systémů PZTS tak, aby byl systém PZTS vhodný pro prostor, kterým má být zabezpečen ve vztahu k očekávaným rizikům. Návrh systému PZTS závisí na řadě faktorů, které všechny v menší nebo větší míře návrh PZTS ovlivní. Posouzení těchto faktorů vyústí ve vypracování návrhu systému PZTS odpovídajícího rozsahu, stupně zabezpečení a třídy prostředí.

- **Kapitola 8 – Příprava realizace**

Tato kapitola slouží jako vodítko pro ty, kdo jsou odpovědní za montáž PZTS, a zdůrazňuje faktory, které je třeba vzít v úvahu před zahájením vlastní montáže.

- **Kapitola 9 – Montáž**

V této kapitole jsou uvedena doporučení týkající se problémů, které mohou nastat v průběhu montáže PZTS. Cílem této kapitoly je zajistit, aby PZTS byl namontován v souladu se specifikací obsaženou v návrhu systému.

- **Kapitola 10 – Kontrola provedení montáže, funkční zkouška a převjíčka**

V této kapitole jsou uvedena doporučení k řešení problémů vznikajících po skončení montáže PZTS. Účelem je ujistit se, že byl PZTS namontován v souladu se specifikací a splňuje funkční požadavky vyspecifikované v návrhu systému. Dále jsou uvedeny pokyny pro uvedení do provozu a předání PZTS uživateli a pro zpracování dokumentace, záznamů a návodů k obsluze, které je nutno uživateli předat.

- **Kapitola 11 – Dokumentace a záznamy o provozu systému**

Tato kapitola popisuje dokumentaci, kterou je třeba předat klientovi po dokončení montáže PZTS. Tato dokumentace je určena pro záznamy o historii modifikací PZTS, vycházející

z dokumentace skutečného provedení, zpracované po dokončení montáže PZTS. Záznamy o provozu systému slouží k chronologickému přehledu o jakýchkoli nápravných opatřeních následujících po vyvolání planých poplachů a k poskytnutí informací o jakýchkoli opravách nebo modifikacích PZTS. Záznam má také obsahovat podrobnosti o dočasných selháních systému.

- **Kapitola 12 – Provoz PZTS**

Tato kapitola popisuje odpovědnost klienta nebo uživatele PZTS za pravidelnou údržbu PZTS a za zajištění, správné obsluhy PZTS.

- **Kapitola 13 – Údržba a opravy PZTS**

V této kapitole je uvedeno, jak má být prováděna údržba a opravy systému PZTS, aby byly zajištěny funkční požadavky, definované v jeho návrhu.

Tyto pokyny pro aplikace obsahují pokyny pro navrhování, přípravu realizace, montáž, uvedení do provozu, provoz a údržbu PZTS instalovaných v budovách. Požadavky na systémy PZTS jsou specifikovány v EN 50131-1:2006. Neobsahuje-li systém PZTS funkce, vztahující se k detekci narušení, neaplikují se požadavky vztahující se k detekci narušení. Neobsahuje-li systém PZTS funkce, vztahující se k detekci přepadení, neaplikují se požadavky vztahující se k detekci přepadení [9].

Požární evakuační plány musí být v nemocnici zpracovány pro objekty, kde jsou složité podmínky pro zásah dle §18 vyhl. MV č. 246/2001 Sb. Součástí požárního evakuačního plánu je grafické znázornění evakuačních cest v jednotlivých podlažích, které se umísťují u vstupů do jednotlivých podlaží.

Dokumentace požární ochrany je podkladem pro zajištění požární ochrany, průkazným materiálem pro dozorové orgány.

Požární poplachové směrnice nemocnice vymezují činnosti zaměstnanců a dalších osob zdržujících se v areálu nemocnice při vzniku požáru. Vymezují způsob vyhlášení požáru včetně postupu při vzniku požáru. Jsou umístěny v objektu na viditelných místech. Všichni zaměstnanci musí být seznámeni s požárními poplachovými směrnicemi vstupní instrukcemi při nástupu do pracovního poměru a pak opakovaně dle platných nařízení. Požární



poplachové směrnice jsou jedenkrát ročně revidovány a prověřovány cvičným požárním poplachem.

Dokumentací požární ochrany nemocnice je dokumentace o začlenění do kategorie činností se zvýšeným požárním nebezpečím, stanovení zabezpečení požární ochrany, požární kniha, požární poplachové směrnice, požární řády, požární evakuační plán, dokumentace zdolávání požáru, tematický plán a časový rozvrh školení a odborné přípravy o požární ochraně, dokumentace o školení a odborné přípravě požární ochrany, písemné zprávy o provedených revizích a kontrolách provozuschopnosti věcných prostředků požární ochrany a požárně bezpečnostních zařízení, zápisy o kontrolních prověrkách orgánů vykonávajících státní požární dozor, povinnosti zaměstnanců v případě vzniku požáru, přehled o požárech, seznam udělených vyjímek a dokumentace obsahující podmínky požární bezpečnosti. Dokumentaci požární ochrany zpracovává odborně způsobilá osoba a je soustředěna v kanceláři technika požární ochrany a vedoucích zaměstnanců. Plnění úkolů požární ochrany je v nemocnici zajištěno smluvně s externí firmou zabývající se touto problematikou jež plní i funkci technika požární ochrany.

### 3 ANALÝZA RIZIK V OBJEKTOVÉ BEZPEČNOSTI

Bezpečnostní analýzou objektu provádíme bezpečnostní posouzení, topografii předmětu střežení a režimovou studii objektu. Analyzovány jsou všechny části objektu a subjekty v tomto objektu nacházející.

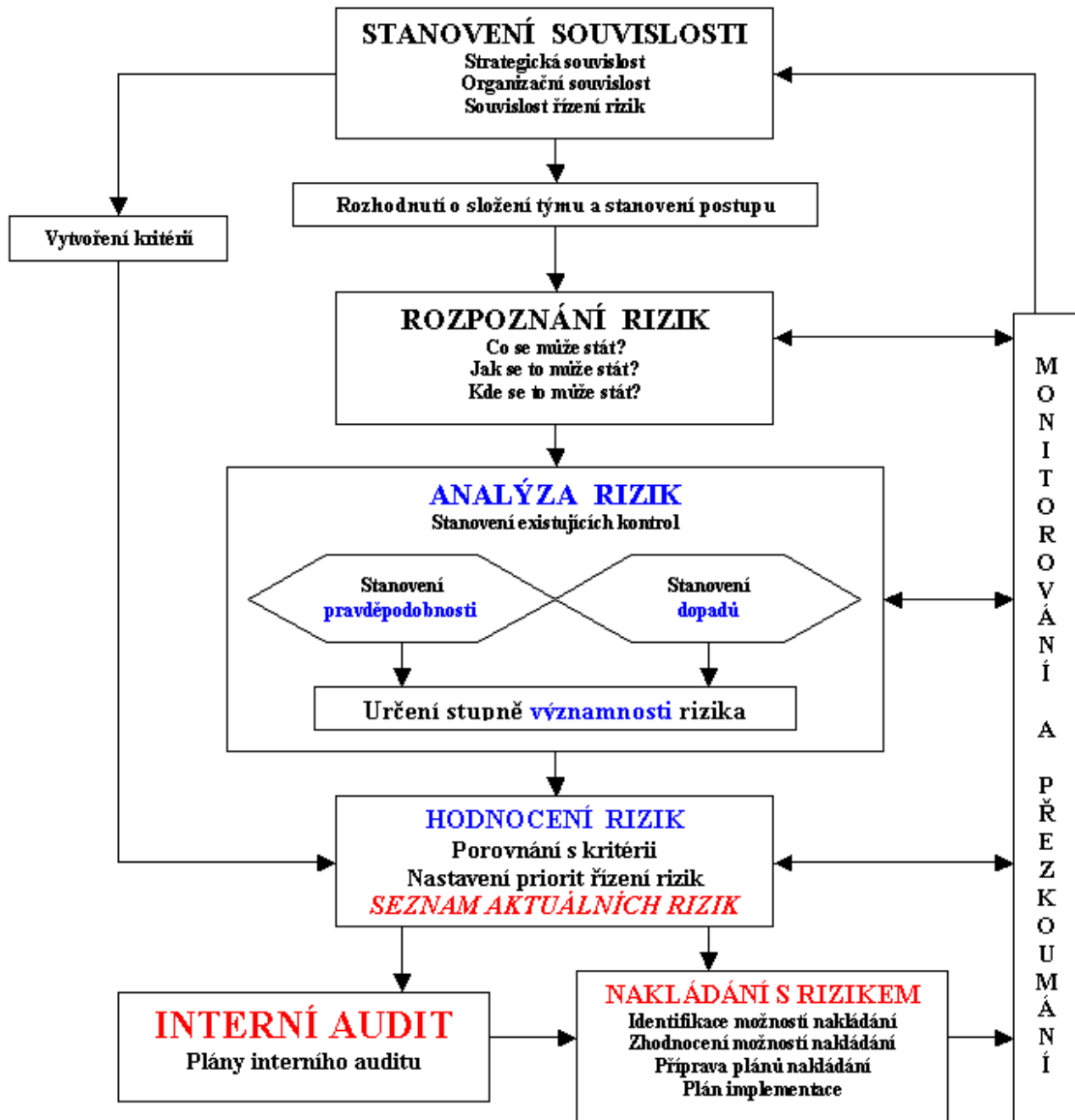
Bezpečnostní analýza soustřeďuje popis objektu, prověrku lokality budovy, režimovou studii objektu, porovnání projektu PZTS s režimy ostrahy objektu, seznam a popis nebezpečí, možné způsoby napadení objektu, přehled zranitelných míst a vnější vlivy. Popis objektu ochrany je posouzení rozsahu a charakteru majetku vystaveného ve střeženém objektu nebezpečí. Prověrka lokality budovy znamená posouzení budovy střeženého objektu (konstrukce pláště, poloha střeženého objektu, personál, držení klíčů, stávající zabezpečení, historii krádeží, předpisy a vlivy působící na PZTS). Režimovou studii objektu je pohyb osob v pracovní i mimopracovní době. Možné způsoby napadení objektu se určují ze stanovených druhů nebezpečí ohrožujících chráněný zájem a definují se způsoby napadení objektu a následně kritická (zranitelná) místa [10].

Integrovaný bezpečnostní systém se skládá z propojených prvků mechanických zábranných systémů tj. klasická ochrana, signalizačních a monitorovacích prostředků tj. technická ochrana a systému organizačních opatření a ostrahy, což je režimová a fyzická ochrana [11].

Klasickou ochranou se rozumí v širším pojetí zeď, okna, dveře, střecha, ale i podlaha objektu. V užším pojetí jsou to mechanické zábranné prostředky jako jsou bezpečnostní skla, trezory, bezpečnostní fólie, uzamykací systémy nebo bezpečnostní schránky. Smyslem této ochrany je ztížit případně úplně zabránit narušiteli dostat se do chráněného prostoru. Mechanické zábranné prostředky se dále rozdělují podle toho, které části objektu chrání. Jedná se o prostředky obvodové ochrany, prostředky plášťové ochrany a prostředky předmětové ochrany [11].

Technická ochrana je tvořena prvky signalizačního a monitorovacího systému, které představují elektronické zařízení a prostředky. Tyto registrují a předávají informace o napadení chráněného objektu. Jsou to pulty centralizované ochrany, elektrické požární systémy, PZTS, kamerové monitorovací systémy, prostředky perimetrické ochrany, prostředky ochrany dat a informací, individuální technické prostředky, přepěťovou ochranu a speciální ochranu. Celkově podporují klasickou a zefektivňují fyzickou ochranu [11].

K pravidelnému zjišťování možných rizik v Nemocnici Břeclav dochází pomocí interních auditů, jež provádí školení interní auditoři. Principy řízení rizik a základní postupy popisuje následující schéma.

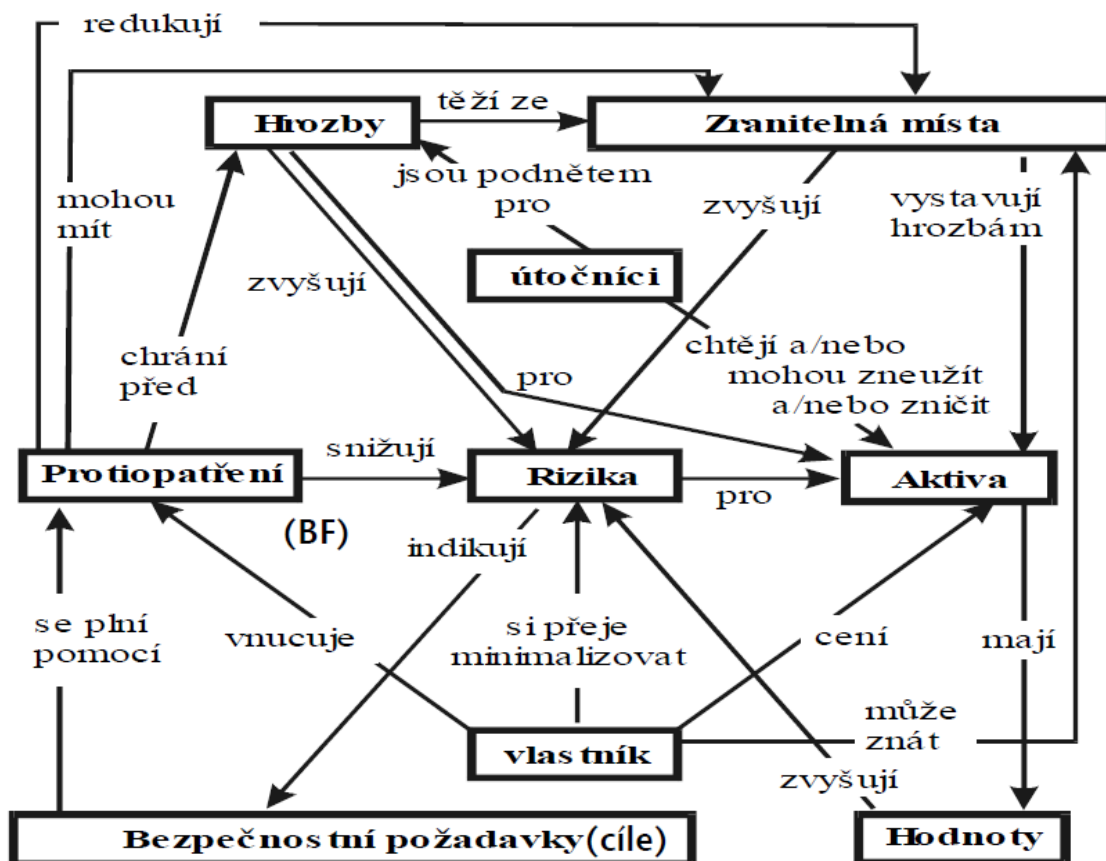


Obr. 1. Principy řízení rizik a základní postupy [17]

Aby plán řízení rizik zůstal stále aktuální, je třeba jej upravovat na základě posouzení aktuálního stavu. Podmínky, které mohou ovlivnit následky a jejich pravděpodobnosti, se mohou změnit, stejně jako okolnosti, které ovlivňují náklady nebo vhodnost různých přístupů ke zvládnání rizik. Proto je nutné cyklus řízení rizik pravidelně opakovat.

Sledování a posuzování přinášejí také poučení z probíhajícího procesu řízení rizik prostřednictvím hodnocení událostí, plánů zvládnání rizik a jejich výsledků.

Základní bezpečnostní pojmy a vztahy jsou znázorněny na obrázku č. 2, kde cílem je chránit hodnoty. Předpokladem je eliminace zranitelných míst či hrozeb a pečlivá kontrola bezpečnostních systémů a opatření.



Obr. 2. Základní bezpečnostní pojmy a vztahy [27]

Pokud organizace využívá více prvků ochrany je žádoucí integrace tedy vzájemné propojení těchto systémů, čímž se zvýší komfort obsluhy takového komplexního systému, centralizuje správa, minimalizují se časové náklady na řízení systému, zvýší se kvalita a sníží náklady spojené se zajištěním ochrany bezpečnosti. Cílem komplexního zabezpečení objektu je vytvořit bezpečnostní komplex. Bezpečnostní komplex je souhrnem organizačních a technických opatření spojených v jeden celek. Součástí komplexu jsou systémy kamerové, docházkové, přístupové, zabezpečovací a ovládací prvky jako jsou osvětlení, vytápění, vzduchotechnika, klimatizace apod. V takovém komplexu jsou tyto

systemy technicky a logicky provázané. Zvyšuje se účinnost jednotlivých systémů což umožňuje centralizovaná správa všech událostí. Propojení třeba kamerového systému s pohybovými detektory zabezpečovacího systému umožní ukládání záznamů pouze v době událostí čím se odbourává nutnost pořizování nepřetržitého záznamu. V nočních hodinách může být běžné osvětlení vypnuté a zapínat se podle signálů vnějšího zabezpečovacího okruhu nebo na povel přístupového systému z otevřených dveří, brán či závor.

Elektronická požární signalizace jsou systémy, které mají za úkol včasnou detekci případně prevenci vzniku požáru. Použití takových systémů je rozsáhlé a finančně náročné, ale ve vztahu k hodnotám, které nepřetržitě chrání je to náklad opodstatněný a užitečný. Jedná se o plně automatické systémy, které dále varují osoby nacházející se v ohrožené lokalitě, upozorňují na vzniklé nebezpečí i další vytyčené osoby případně složky hasičského záchranného sboru.

Teoretická část diplomové práce umožnila vytvořit znalostní základnu, která relevantně ohraničila zkoumaný problém. Vytvořený teoretický rámec umožnil objektivnější formulaci těch skutečností, které je možno vnímat z pohledu vypracování praktické části práce.

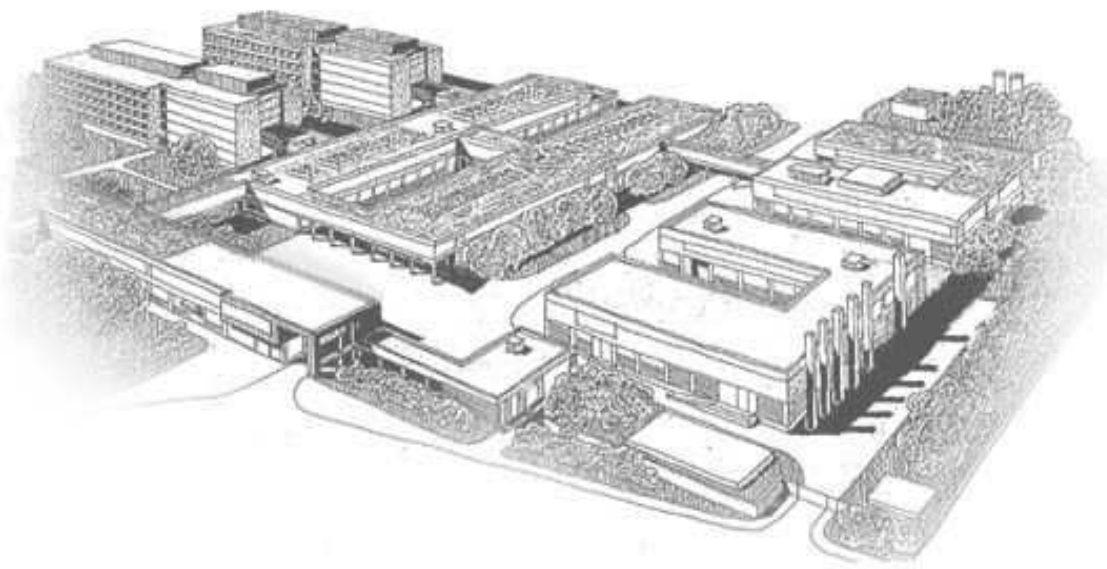
## **II. PRAKTICKÁ ČÁST**

## 4 NEMOCNICE BŘECLAV

Nemocnice Břeclav je příspěvkovou organizací jejímž zřizovatelem je Jihomoravský kraj jako samosprávný celek. Patří mezi nejvýznamější zaměstnavatele v regionu, pracuje zde více jak 600 zdravotnických pracovníků a hospodářsko-technické a administrativní činnosti zajišťuje více jak 100 zaměstnanců. V čele stojí ředitel, který je jmenován zřizovatelem tj. Krajský úřad Jihomoravského kraje v Brně. Řídí veškerou činnost nemocnice a jeho příkazy jsou pro všechny pracovníky závazné.

Nemocnice Břeclav je všeobecnou nemocnicí tzv. okresního typu, s rozsáhlou lůžkovou i ambulantní složkou, poskytující diagnostickou, léčebnou a ošetrovatelskou péči pro spádovou oblast až 130 tisíc obyvatel. Dále se podílí na průběžném vzdělávání zdravotnických pracovníků a praktické výchově posluchačů lékařských fakult a studentů zdravotnických škol.

Snaha o neustálé zvyšování kvality péče, kontinuity a koordinace všech činností vedla management nemocnice k zavedení integrovaného systému řízení jakosti, environmentu a bezpečnosti práce. Nemocnice je v současné době držitelem certifikátů dle mezinárodních norem ISO 9001, ISO 14 001 a OHSAS 18 001.



Obr. 3. Náčrt areálu Nemocnice Břeclav, p. o. [18]

## 4.1 Historie nemocnice

Areál nemocnice v Břeclavi byl vybrán na strategicky výhodném, v tehdejší době na volném a požadovaně dostatečně velkém pozemku, který zároveň bude v rámci města dostatečně dostupný v rámci infrastruktury. Základní kámen byl položen již v roce 1986, kdy výstavba byla plánována ve dvou etapách. Do roku 1992 byla vybudována první lůžková budova s neoperačními obory a potřebné budovy zázemí tvořící laboratoře, diagnostické oddělení a také zásobování stravou, energiemi, materiálně technickými potřebami apod. Z dochovaných fotografií je patrné, že zabezpečení areálu připomínalo spíše oplocení staveniště.

Ve druhé etapě dokončené v roce 1996 byly vybudovány druhá lůžková část s operačními obory a budovy s operačními sály, centrální sterilizací a ARO. Následně byl vybudován kompletní obvodový plášť pro zajištění prostoru areálu nemocnice. S rozvojem zabezpečovací techniky byly pořízeny první monochromatické kamery monitorující pohyb na parkovišti pro zaměstnance a zadní vjezd pro vozidla, který byl provozován v případech stavebních úprav pro vjezd těžké techniky a vozidel IZS.

Ostrahu areálu zajišťovalo postupně několik soukromých bezpečnostních agentur. Zabezpečovaly fyzickou ostrahu objektu a registrovaly vjezd vozidel a osob přes vrátnici nemocnice.

Co se provozu nemocnice týkalo byla součástí areálu i spalovna, která splňovala tehdejší platné legislativní normy a byla využívána převážně ke spalování vlastního odpadu. Po bezpečnostní stránce představovala velmi nízké riziko nebezpečí protože veškerý provoz byl pod přísným dohledem proškolených pracovníků a dozorových orgánů samosprávy.

Po roce 2003 byl provoz spalovny zastaven. Poslední část komplexu nemocnice Mezioborová jednotka intenzivní péče byla dokončena v roce 2012, kdy byla také nemocnice kompletně zkolaudována.

## 4.2 Současná nemocnice

Nemocnice Břeclav je všeobecným zdravotnickým zařízením s lůžkovými odděleními poskytující diagnostickou, ošetrovatelskou a léčebnou péči pro spádovou oblast s více jak 100 tisíci obyvateli. Nabízí rozsáhlé lůžkové i ambulantní složky sjednaných



zdravotnických oborů. Zabezpečuje poskytování zdravotnických služeb i obyvatelům mimo vlastní spádovou oblast v rámci svobodné volby lékaře. Dále poskytuje konzultační a vzdělávací činnosti v oboru zdravotnictví. Zajišťuje dostatek transfuzních přípravků zpracování krve bezplatných dárců, lékařskou službu první pomoci v rozsahu stanoveném příslušnými právními a jinými požadavky, smlouvami s jednotlivými zdravotními pojišťovnami a jinými plátcí zdravotní péče s nadregionální působností. Poskytuje druhy zdravotní péče podle časové naléhavosti jejího poskytnutí v rozsahu neodkladná péče, neodkladná péče v případech hromadného neštěstí, akutní péče, nezbytná péče o pacienty, plánovaná péče. Podle účelu poskytnutí jsou dále druhy zdravotní péče v nemocnici poskytovány jako preventivní, diagnostická, dispenzární, léčebná posudková, léčebně rehabilitační, ošetrovatelská, paliativní a lékárenská péče.

Plní podle zvláštních předpisů a směrnic úkoly spojené se zabezpečením zdravotní péče při obecném ohrožení. Nemocnice se dělí dle druhu činnosti na oddělení a útvary (úseky) v souladu s organizačním řádem. Oddělení jsou mezi sebou vzájemně pracovně propojena. Pro všechny vykonávané činnosti jsou stanoveny odpovědnosti, pravomoci a vzájemné vztahy.

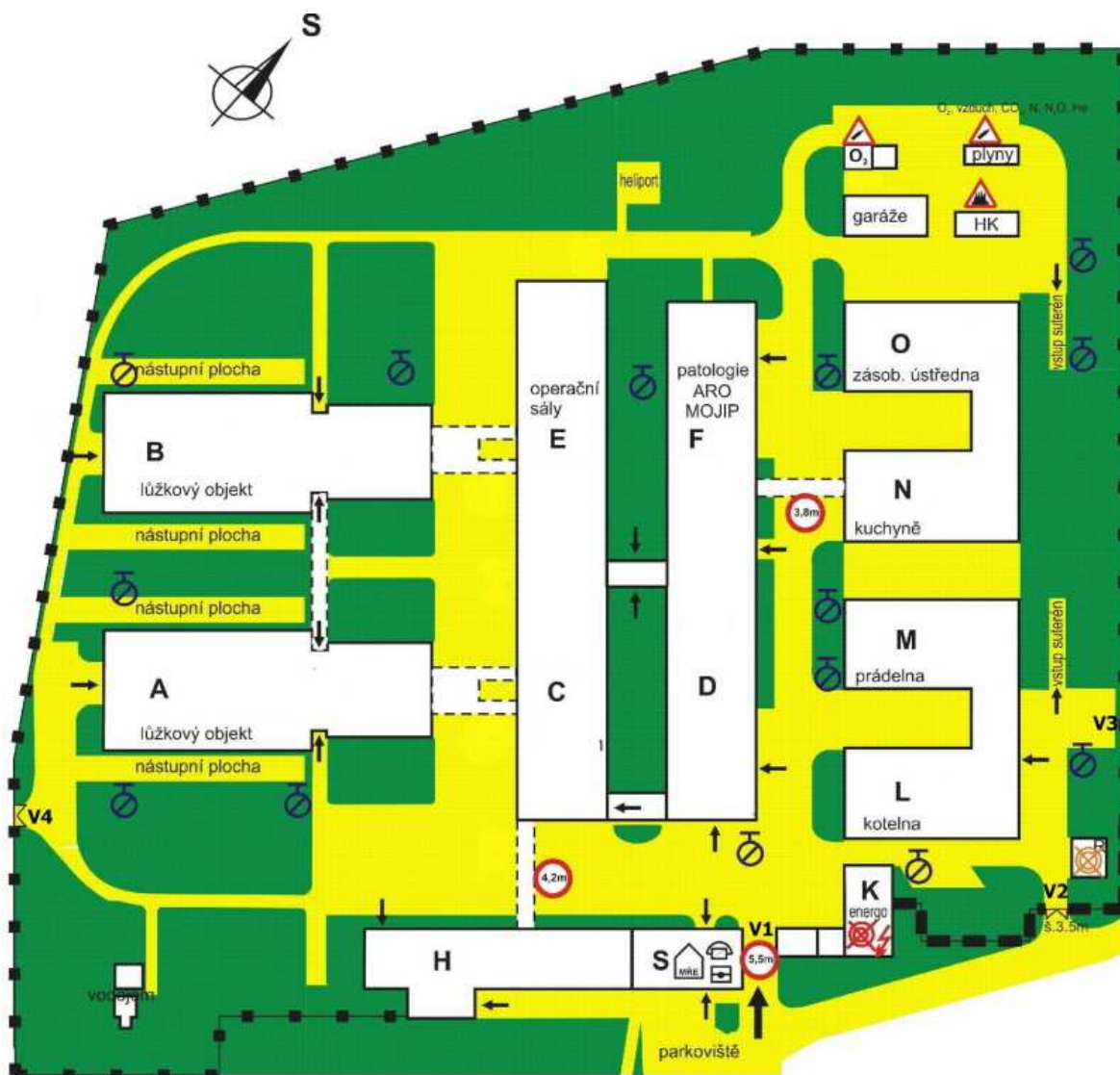
Organizační struktura nemocnice se skládá z vrcholového managementu pod vedením ředitelky nemocnice, ekonomické náměstkyně, náměstkyně léčebně preventivní péče, hlavní sestry, představitelky vedení QMS a představitele pro EMS, HSMS. Dále sem patří zdravotnická část se 22 medicínskými odbornostmi, z toho je 12 lůžkových oddělení, 4 specializované laboratoře, administrativní pracoviště a úseky hospodářsko-technické.

Od roku 2004 zajišťuje ostrahu objektu oddělení správy a údržby pomocí vlastních pracovníků vyškolených pro fyzickou ostrahu osob a objektu. V kompetenci těchto osob je evidence vozidel při vjezdu.

Ve velkých a rozsáhlých objektech hrozí riziko fyzického napadení, krádeží cenných předmětů. V případě nemocnic zcizení třeba léků a zdravotnického materiálu, únosů hospitalizovaných osob či zaměstnanců.

Uvnitř areálu jsou důležité hlavní komunikační a spojovací chodby v nichž dochází k velkému pohybu osob. V případě krizové situace mají tyto transportní chodby sloužit jako shromaždiště pacientů lůžkových oddělení, personálu a oprávněných osob.

Nemocnice se rozkládá na rozsáhlém pozemku nedaleko centra města Břeclavi, ale přitom v okrajové části mezi hlavním tokem řeky Dyje a jeho odlehčovacím ramenem. Obvod celého pozemku je více jak jeden kilometr dlouhý a obepíná jej z větší části drátěný plot a dále budovy přiléhající k hranicím pozemku.



Obr. 4. Plán areálu nemocnice [29]

Uvnitř areálu jsou dvě hlavní pěti podlažní lůžkové budovy, budovy vyšetřovacích složek a laboratoří, budovy administrativní a také budovy materiálně technického zabezpečení a heliport pro možnost přistání a odletu helikoptéry. V okrajových částech jsou důležité zásobovací prvky jako zásobník kapalného kyslíku, zásobník pitné vody, regulační stanice, energoblok a sklady technických plynů.

Do rozsáhlých areálů ústí zpravidla více jak jeden vjezd pro vozidla a tyto jsou hlavním kontaktním místem pro ostrahu objektu. Je nutnost řešit dopravní situaci v areálu, parkovací plán a vytyčit místa důležitá k případné evakuaci v případě nutnosti opuštění objektů.

Do areálu je možnost vstupu hlavním vchodem nebo bočním vstupem z parkoviště pro zaměstnance. Vjezd do objektu je možný hlavním vjezdem zajištěným ostrahou objektu a elektricky ovládanou závorou, zadní branou pro případný vjezd vozidel IZS a nakonec boční vjezdovou branou s odsuvnou zábranou, která slouží pro případ neprůjezdnosti hlavním vjezdem nebo při poruše elektrické závory hlavního vjezdu.

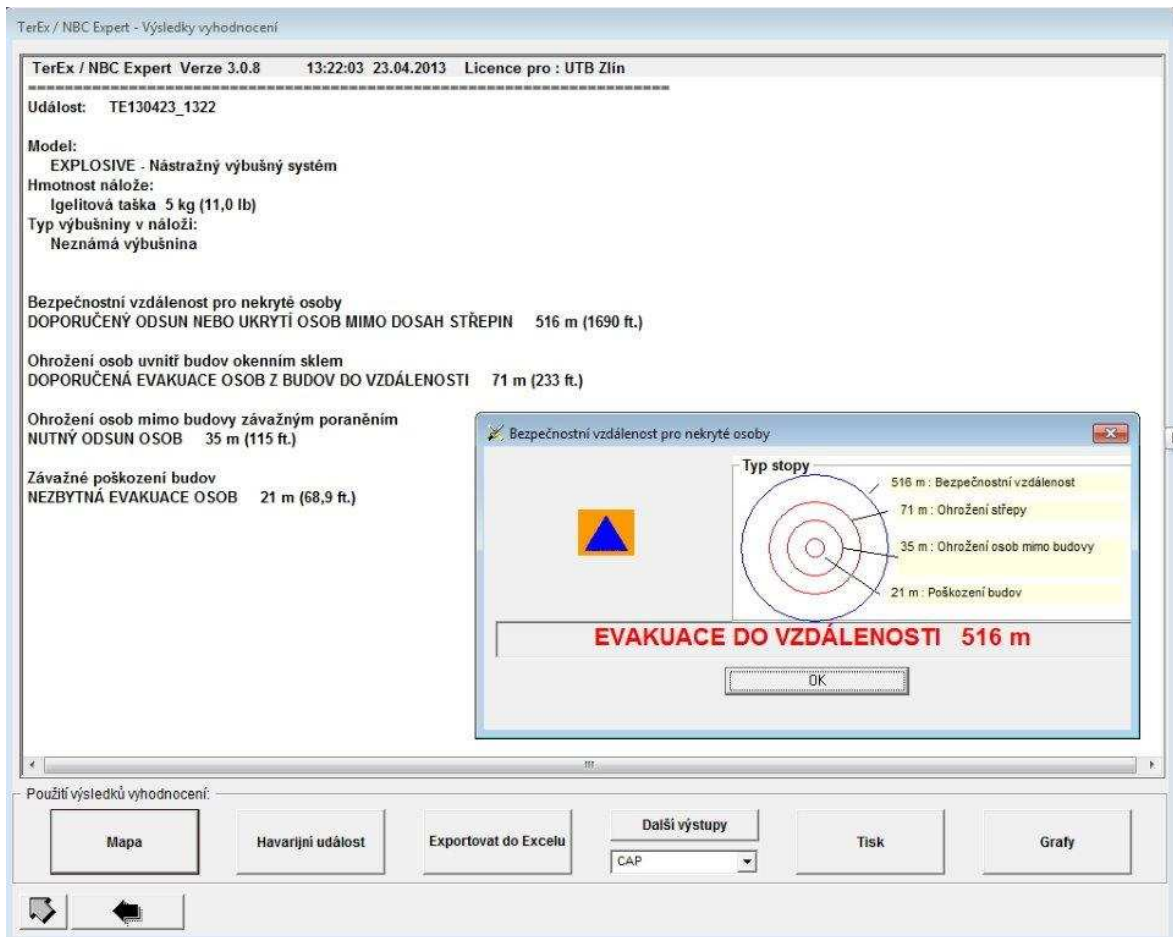
Jako jeden z posledních komunikačních prostor nemocnice je možné počítat heliport, který byl původně před vstupní budovou, ale po získání dostatečných finančních prostředků byl v zadní části areálu vybudován plnohodnotný prostor pro přistávání helikoptér většinou odvázejících pacienty k náročnějším zákrokům do specializovanějších zdravotnických zařízení. Funguje však v případě mimořádné události také jako heliport pro případné zásahy IZS apod.

## 5 BEZPEČNOSTNÍ ANALÝZA

Objekt nemocnice patří mezi zařízení s možností výskytu bezpečnostních rizik, proto je nutné analyzovat všechny přímé i potencionální hrozby a navrhnout vhodná protiopatření. Dle mých zjištění však chybí v areálu komplexní řešení a modernější vybavení zabezpečovací technikou.

Místostrahy je u hlavního vchodu a strážný při výkonu služby zpravidla stojí u vchodu, aby měl lepší vizuální kontakt s osobami procházejícími tímto místem. Může tak dojít k fyzickému **napadení ostrahy** a její omezení ve výkonu služby.

Dalším takovým rizikem je **hrozba umístění nástražného výbušného systému** v blízkosti objektu nebo uvnitř budov nemocnice.



Obr. 5. Ukázka účinku NVS uloženého v igelitové tašce [30]

Povědomí o takových zařízeních díky elektronizaci komunikace a dostupnost internetu zvyšuje riziko takových situací. Následkem takového činu by mohly být i situace významného ohrožení rutinního provozu nemocnice a poškození budov.

Zasažení takovým systémem by bylo úměrné místu uložení. Pokud by došlo k nástraze v odlehle budově nízkého provozního významu nebyly by následky tak ohrožující. Došlo-li by k nástraze v budově zásobování nebo její blízkosti mohlo by dojít k narušení běžného chodu nemocnice a bylo by nutno zajisti hlavně náhradní plán zásobování danou komoditou pro znovuoobnovení provozu. V případě uložení nástražného výbušného systému do budovy lůžkových oddělení by pravděpodobně došlo ke kritickým situacím, které by vyžadovaly zásah bezpečnostních složek státu. Známý jsou hlavně plané poplachy o umístění nástražných výbušných systému, které však vyžadují bezpečnostní situaci jako by se jednalo o pravdivou výhružku a to až do doby zjištění skutečného stavu.

V současné době je riziko terorismu stále aktuálnější a proto musí být každá veřejná instituce obezřetná. **Teroristický útok** představuje riziko spojené s jednáním osob, které se snaží na sebe upozornit s použitím hrubého zastrašování s cílem vystrašit co nejvíce osob. Projevuje se často zadržováním rukojmí, vraždami, únosy osob, vydíráním nebo vyhrožováním.

Hrozbou současné doby je stále i **vandalismus** spojený s poškozováním a ničením majetku pachateli. Následky takového jednání vyžadují nemalé výdaje na obnovení poničených hodnot.

Mezi další možná vnější rizika patří možnost **napadení skupinou pachatelů**, kteří by mohli jak ničit vybavení nemocnice, ohrozit pacienty ambulantní i hospitalizované nebo napadnout pracovníky ostrahy.

Vnitřní rizika jsem analyzoval na základě zjištění ze zápisů z provozních knih a konzultací s vedoucím hospodářsko-technického úseku, vedoucím ostrahy, správce systému elektrické požární signalizace, pracovnice interního auditu a vedoucího oddělení informatiky a telekomunikací.

Při výkonu ostrahy může za určitých situací dojít k **selhání fyzické ostrahy** at' z důvodu nepozornosti, zdravotních příhod nebo jiných kolizních situací.

Důležitým rizikem by mohl být **výpadek funkce EPS** s návazností na možnost vzniku požáru v objektu s velkým množstvím osob. Avšak v situaci kdy by nehrozil požár tedy při stálém dodržování protipožárních opatření nehrozí vysoké nebezpečí a za předpokladu že dozor EPS neprodleně informuje správce EPS o tomto výpadku.

Naproti tomu případný **výpadek funkce PZTS** by mohl mít za následek širší a tím pádem významější bezpečnostní riziko.

**Krádež** zdravotnické dokumentace nebo důležitých dokumentů organizace by mohl ohrozit zdraví či životy osob nebo by mohla vážně narušit provoz organizace.

**Použití biologické, radiologické či chemické látky** k poškození zdraví či života osob nacházejících se v objektu by mohla velmi vážně ohrozit dotčené osoby a provoz poskytování lékařské péče.

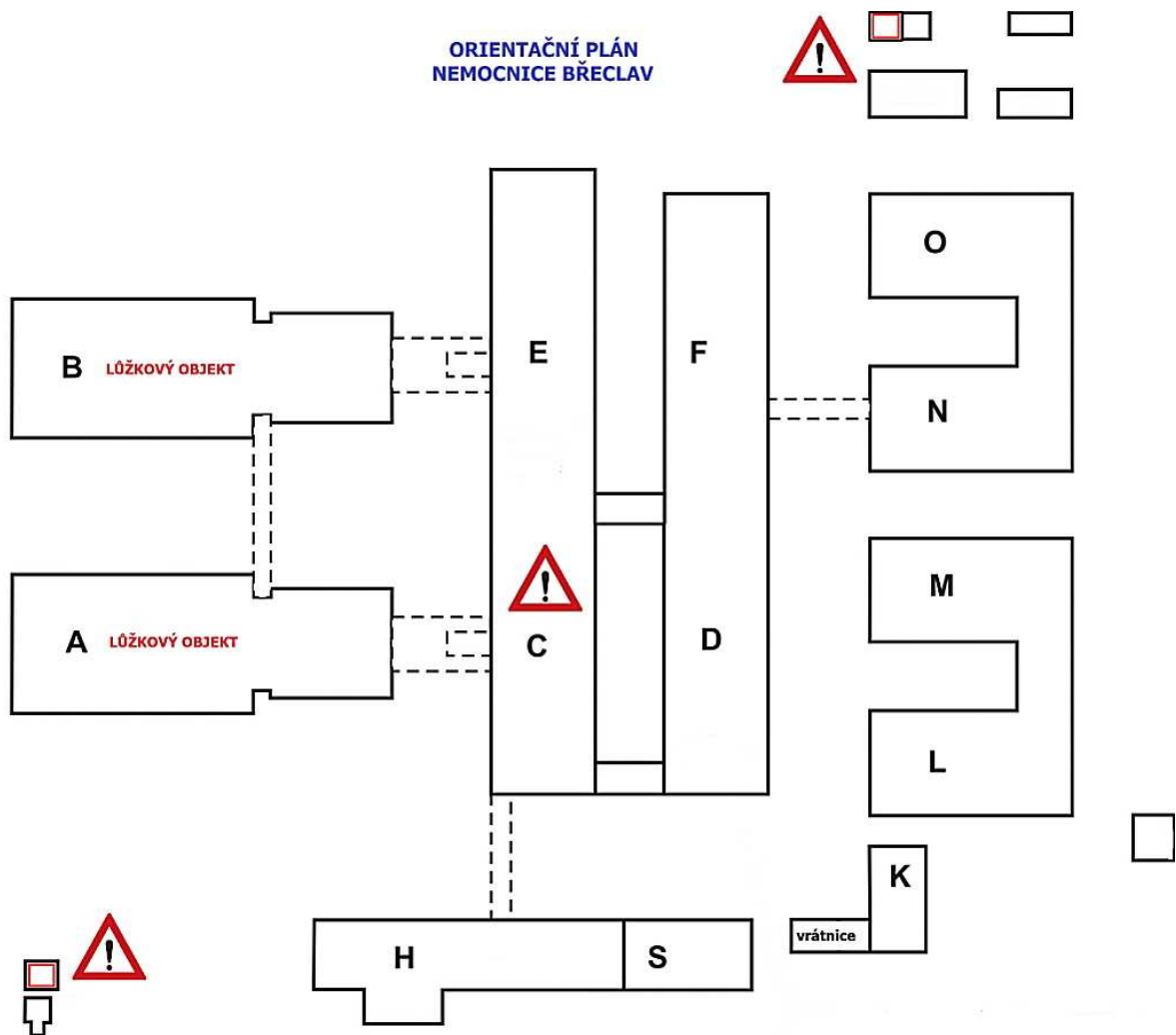
**Únik elektronických dat** organizace by mohl nejvíce ohrozit provoz nemocnice a tím narušit bezpečnost objektu a osob v něm. Je proto nutné dodržovat veškeré postupy v rámci administrativní bezpečnosti.

V dalších krocích bezpečnostní analýzy jsem posuzoval situační plán areálu se zaměřením na riziková místa v jednotlivých částech objektu.

Dominantou areálu jsou dvě lůžkové budovy, které jsou vybaveny řádně veškerou protipožární technikou včetně elektronicky řízených uzavíratelných vstupů, detektorů i mechanických hlásičů požáru. Vznik požáru je totiž nejvyšší riziko v těchto budovách s ohledem na dodržování všech protipožárních předpisů. Každodenní rutinní provoz ve zdravotnickém zařízení vyžaduje používání desinfekčních prostředků a podobných chemikálií.

Proti vniknutí do těchto budov jsou vybaveny zadní a boční vchody uzamykatelnými prosklenými dveřmi s bezpečnostní fólií. Vstupní čelní dveře jsou řízeny senzoricky detektorem pohybu, kde pro případ výpadku elektrické energie jsou po stranách umístěny záložní uzamykatelné dveře. Pohyb osob je možný po schodištích, která slouží i pro případ evakuace a jsou umístěna v krajních částech budov i uprostřed, které jsou určeny pro volný pohyb osob i zdravotnického personálu. Stejně tak pro přesun vozíků, lehátek a podobných pohyblivých zařízení jsou určeny výtahy v blízkosti schodišť. Pouze

vyhrazené výtahy však splňují parametry výtahu určeného k evakuaci osob. Jednotlivá lůžková oddělení v rámci poschodí jsou vybavena dvěma vstupy. Tyto mají vícero významů a omezení. Zadní vstupy jsou převážně určeny k zásobování a odvozu spotřebovaných materiálů a také k transportu zemřelých. Tyto zadní vchody jsou zpravidla vybaveny plnými dveřmi s atypickou klikou a cylindrickým zámekem, aby byl znemožněn samovolný vstup na lůžkové oddělení. Přední vstupy jsou vybaveny prosklenými dveřmi s madly, které nejsou uzavřeny nebo zajištěny před volným otevřením což umožňuje nekontrolovaný pohyb osob v denních hodinách.



Obr. 6. Situační plán nemocnice s vyznačením rizikových míst

Ze situačního plánu nemocnice s vyznačením rizikových míst je patrné, že takových míst v objektu naštěstí není mnoho. Mezi tato riziková místa patří pozemní zásobník kapalného kyslíku s nebezpečím výbuchu, pracoviště radiologicko-diagnostického oddělení s výskytem ionizačního záření a v neposlední řadě vodojem se zásobníkem pitné vody pro celý objekt. Narušením bezpečnostních opatření v těchto místech by mohlo dojít k nejzávažnějším přímým ohrožením zdraví a života osob v areálu tedy jak zaměstnanců tak hlavně hospitalizovaných pacientů a v pracovních dnech samozřejmě také pacientů ambulantních. Všechny tyto místa jsou vyznačena výstražnými tabulkami s odpovídajícími symboly vyobrazujícími riziko nebezpečí v konkrétním případě. Omezený pohyb osob v takových místech snižuje riziko vzniku mimořádné události. Stejně tak pravidelná povinná školení zodpovědných osob a zaměstnanců, kteří docházejí do styku s rizikovými místy při výkonu svého povolání minimalizují všechna známá rizika.

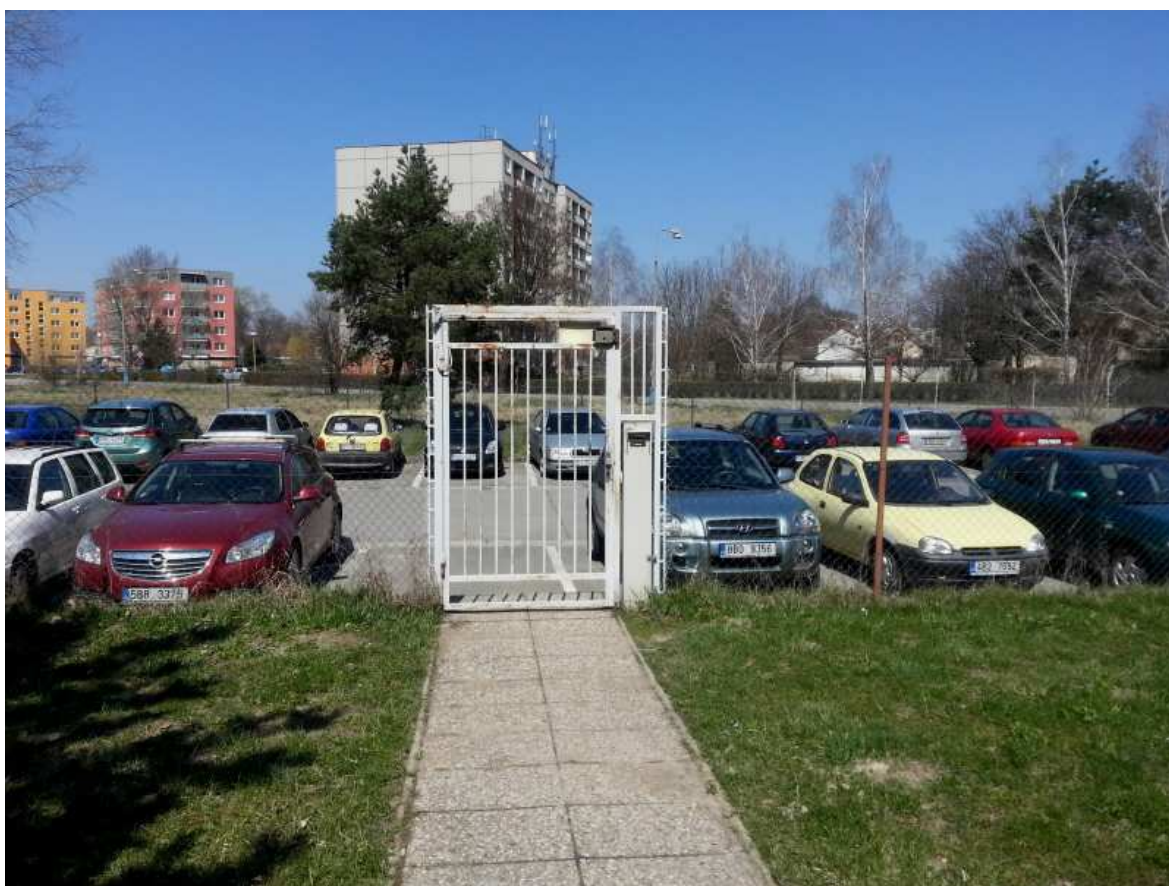


Obr. 7. Pozemní zásobník kapalného kyslíku monitorován pomocí CCTV



Nejstřeženější oblasti areálu jsou pod neustálým dohledem kamerového systému a je monitorován pohyb osob v blízkosti těchto míst. Je zapotřebí neustálého dodržování všech bezpečnostních opatření a zjišťování možných rizik. Veškerá opatření pro minimalizaci bezpečnostních rizik jsou vyžadována s ohledem na množství osob pohybujících se denně v areálu nemocnice. Následky vniklé krizové situace by měly hluboký dopad na provoz zařízení a okolních budov.

Právě **pozemní zásobník kapalného kyslíku** patří mezi nejstřeženější objekty a proto je pod neustálým dohledem kamer (viz. obrázek č. 7). Okolí zásobníku je oploceno a opatřeno varovnými tabulkami. Ze zásobníku jsou vytvořeny po areálu mezi jednotlivými budovami rozvody kyslíku pro lékařské využití opatřeny bezpečnostními ventily.



Obr. 8. Vstupní brána ze zaměstnaneckého parkoviště

Mezi slabá místa patřil boční vstup do areálu z parkoviště zaměstnanců a to tím, že nebyl střežen žádnou kamerou CCTV instalovaného v dřívější době. Brána určena pro vstup zaměstnanců pomocí osobního čipu kombinovaného pro otevírání závory ke vjezdu na parkoviště a otevření vstupní brány neplnila tuto funkci.

Mohlo tak docházet ke vniknutí neoprávněných osob nestřeženým vstupem do míst kde je volný vstup k důležitým objektům v areálu nemocnice. Po zjištění tohoto bezpečnostního rizika jsem toto konzultoval s vedoucím hospodářsko-technického oddělení a navrhnul řešení této situace. Bylo provedeno zaměření tohoto místa kamerovým systémem a je plánována modernizace přístupového systému, která bude mít za následek vpuštění do objektu pouze oprávněných osob na základě osobního čipu nebo přístupové karty.



Obr. 9. Oplocení objektu nemocnice s instalovaným kamerovým systémem

Pro fyzickou ochranu objektu nemocnice je použit drátěný plot a obvodové stěny přilehlých budov. Na vybraných místech jsou umístěny kamery pro sledování vyhrazených prostor. Plot je pravidelně kontrolován ostrahou a případná zjištění nestandardního stavu či

narušení jsou zaznamenávána do provozního deníku. Pro vyšší zabezpečení doporučuji modernizaci oplocení a vyznačení varovnými tabulkami, že jde o střežený objekt.

## 5.1 Zabezpečení objektu

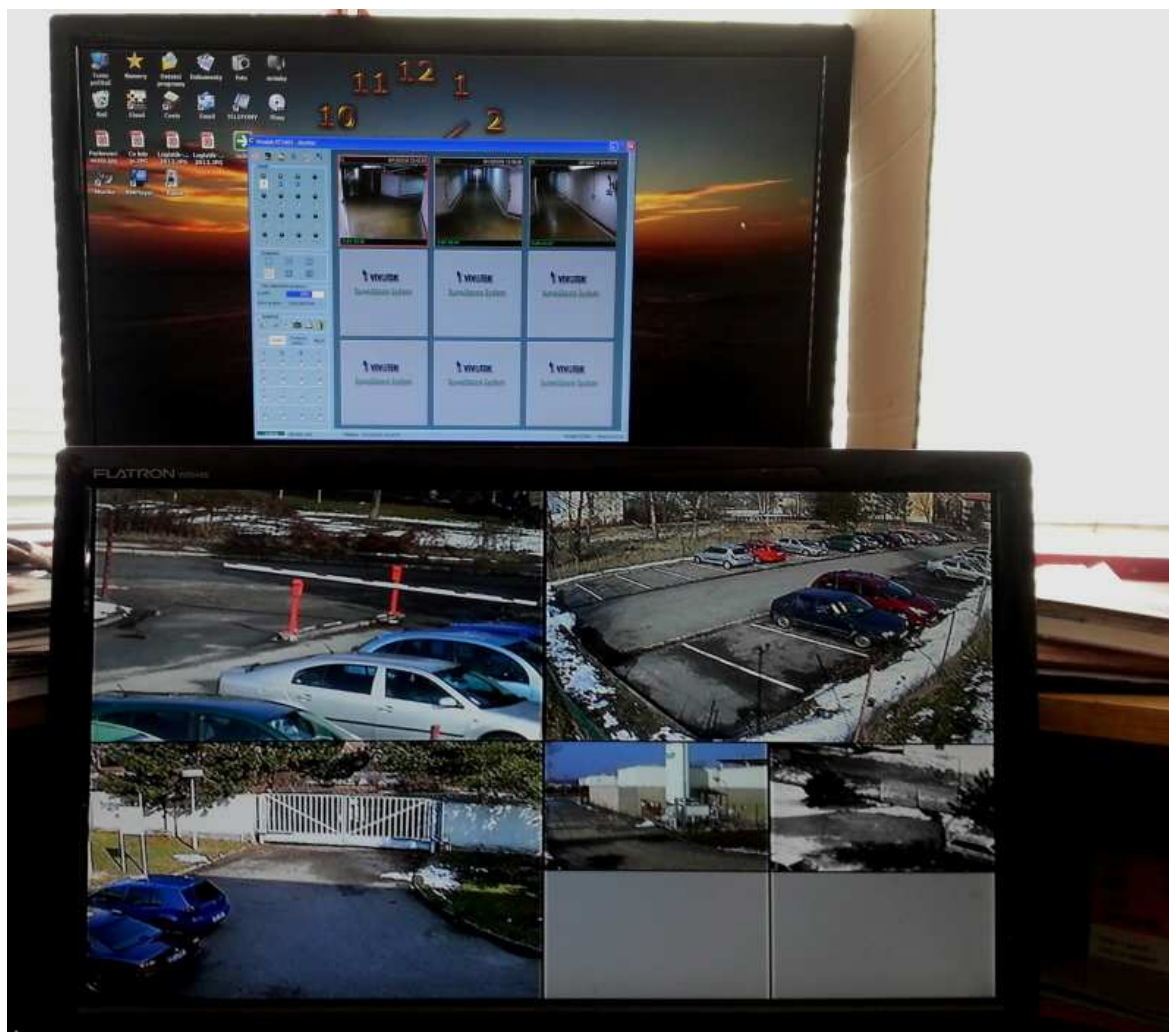
Lůžkové objekty jsou postaveny ze železobetonové konstrukční soustavy. V lůžkových objektech jsou provedeny chráněné únikové cesty a evakuační výtahy. Ostatní objekty jsou postaveny z konstrukční soustavy MS-OB s vyzděním z porobetonových respektive cihelných bloků. V objektu C se v 1. nadzemním podlaží nachází rentgen s možností výskytu radioaktivního materiálu. Objekty v hospodářském dvoře jsou všechny jednopodlažní, zděné a jsou v nich garáže, příruční sklady hořlavých kapalin a sklady mediaplynů jako O<sub>2</sub>, N<sub>2</sub>O, He, vzduch, CO<sub>2</sub>, N<sub>2</sub> a zvláštní směsi. Objekt trafostanice je jednopodlažní a je zajištěn proti vniknutí neoprávněných osob. Obvodový plášť je nehořlavý, montovaný, částečně zděný kde příčky jsou cihelné. Venkovní odpařovací stanice kyslíku o obsahu 6 tun – otevřené technologické zařízení. Roční produkce je do 60 tun O<sub>2</sub>. Transportní chodby jsou v 1. podzemním podlaží a slouží jako dopravní komunikace spojující podzemí lůžkových objektů, kuchyně, prádelnu, společné vyšetřovací a léčebné složky, energoblok a instalační chodby. Vzduchotechnické zařízení je na rozhraní PÚ vybaveno požárními klapkami. Samočinné odvětrávací zařízení v objektech není instalováno.

Veškerá data týkající se pacientů je nutno považovat za důvěrné a musí s nimi být po celou dobu takto nakládáno. Po skončení nutnosti archivace musí být data či dokumentace smazána či skartována. Povinnost zaměstnanců o zachování mlčenlivosti a ochrany dat před zneužitím, odcizením a ztrátou je stanovena v Pracovním řádu a Organizačním řádu organizace v rozsahu dle funkčního zařazení, stanovených odpovědností a náplní práce. Osobní a citlivé údaje pacientů mohou být použity a dále zpracovány pouze v souvislosti s poskytovanou zdravotní péčí. V nemocnici jsou stanoveny bezpečnostní postupy povolující pouze oprávněným osobám získat přístup k datům a informacím. Rozsah přístupu k datům v elektronické podobě je stanoven a zajištěn jednotlivými programy, jež jsou pro zpracování a uchování dat v organizaci používány. Tato opatření jsou pravidelně kontrolována a jsou simulovány krizové situace mající za následek ohrožení informačních systémů a nashromážděných dat.

## 5.2 Výkon ostrahy objektu

Fyzická ostraha objektu plní v zajištění bezpečnosti důležitou roli. Je schopna adekvátně reagovat na každou vzniklou situaci. Mezi každodenní povinnosti strážného patří provádění ochrany a ostrahy majetku a osob, obsluha technických bezpečnostních prostředků, aplikování právních základů bezpečnostní činnosti, součinnost se složkami integrovaného záchranného systému, kontrola osob a vozidel na vstupech a vjezdech, kontrolní činnost ve střežených objektech a také vedení dokumentace o ostraze, kontrolách a poskytnutých službách. Sleduje pohyb vozidel a osob v areálu nemocnice a řeší případné situace.

Provádí vizuální kontrolu míst sledovaných kamerovým systémem na centrálním monitoru, obsluhují zařízení EPS, odemykají a zamykají vchody, provádí pravidelné bezpečnostní obchůzky, podávají informace pacientům a provádí případný doprovod pacientů. V zimním období udržují určené komunikace, spolupracují s městskou policií a v mimopracovní době provádí odemykání tlakové kyslíkové stanice při dodávce kap. kyslíku. Zaznamenává vjezdy a výjezdy vozidel, kontroluje dodržování parkovacího plánu v areálu a dodržování platnosti parkovacích lístků na parkovišti před nemocnicí. Řeší případné prohřešky dohodou s provozovateli vozidla nebo přivolá městskou policii a předá toto do jejich kompetence. V případě potřeby otevírá dveře centrálního příjmu vozům zdravotnické záchranné služby a provádí kontrolu prostor ubytovny. Dále se podílí na odstraňování případných havárií a na provádění evakuací. Plní také další úkoly dle pokynů investičního technika a vedení nemocnice. Pracovníci v nepřetržitém provozu úzce spolupracují s pracovníkem denní směny a naopak. Pracoviště ostrahy objektu nemocnice je organizačně začleněno do hospodářsko-technického úseku a je podřízeno investičnímu technikovi. Vlastní činnost bezpečnostních pracovníků řídí vedoucí ostrahy. Pracoviště je umístěno v budově ostrahy u hlavního vjezdu do nemocnice. Bezpečnostní pracovník těsně spolupracuje s pracovníky informací nemocnice. Vždy, než odejde z pracoviště ostrahy uvědomí o tom pracovníci na informacích. Při každém odchodu nechá zdviženou závoru, aby nebyl narušen hladký průjezd sanitních vozů.



Obr. 10. Dohledové centrum ostražy nemocnice

Na základě smluvního vztahu provádějí příslušníci městské policie kontroly areálu nemocnice. Doba kontroly prováděná motorizovanou hlídkou trvá cca 15 minut a je prováděna převážně v nočních hodinách. Kontroly se provádí i v soboty, neděle a svátky průměrně 1 až 2 krát za směnu. V případě potřeby je možno hlídku přivolat pomocí telefonu nebo zapůjčeného dálkového ovladače, hlídka přijede zpravidla do 10 minut. Kontroly provedené policií se zapisují do knihy služeb s udáním času příjezdu a odjezdu. Veškeré mimořádné události jsou zapisovány do knihy služeb s udáním času a konkrétním popisem dané situace a do evidence NU. Při zjištění či nahlášení jakékoliv trestné činnosti se uvědomí Policie ČR nebo Městská policie. O mimořádné události neprodleně informují Investičního technika. V mimopracovní době a ve dnech pracovního klidu pracovníci informací a v první pracovní den po události i Investičního technika.

Při pohybu vozidel a osob v areálu nemocnice, jsou všichni účastníci povinni dodržovat obecná pravidla bezpečného provozu, řídit se dopravním značením a pokyny bezpečnostních pracovníků, pohybovat se po vyhrazených komunikacích. Motorová vozidla vjíždí a vyjíždí hlavní branou (V1). Pro vjezdy rozměrných vozidel se používá zadní brána u budovy A (V4), nebo boční brána (V2). Tady je bezpečnostní riziko vjezdu vozidla s nebezpečným nákladem, které by bylo možno odstavit na parkovacím místě v areálu a případně aktivovat nástražný systém apod. Je tedy nutno kontrolovat vozidla vjíždějící do areálu jež by mohla takové látky převážet.

Vjezd (V3) na zaměstnanecké parkoviště je možný pouze pomocí osobního čipu vydaného vedoucím pracovníkem. Seznam vydaných osobních čipů opravňujících k vjezdu je uložen na sekretariátu ředitele. Na parkovišti pro zaměstnance mohou parkovat výhradně vozidla zaměstnanců, kteří mají k dispozici čip na ovládání závory. V případě ztráty čipu či karty, je zaměstnanec povinen tuto nahlásit vedoucímu pracovníkovi oddělení nebo přímo odpovědné pracovníci Zaměstnaneckého oddělení. Zcizený nebo ztracený čip je vyřazen z evidence platných čipů pro případ zneužití. Vjezd a výjezd z parkoviště zvednutím závory, je zabezpečován pouze tímto čipem. Nedílnou součástí čipu je Povolení k parkování s platnou známkou, viditelně umístěné ve vozidle. Pohyb na parkovišti je monitorován bezpečnostním pracovníkem nemocnice, ale nemá statut hlídaného parkoviště.

Vjezd a parkování vozidel hospitalizovaných pacientů jsou možné pouze na základě potvrzení o uhrazení parkovného. Pacient žádá o povolení parkování na pokladně nemocnice, kde pacientovi bude vydán doklad o zaplacení se všemi náležitostmi (nahlásí RZ vozidla, oddělení na kterém bude hospitalizován a předpokládanou dobu hospitalizace, provede úhradu). Pokladna vystaví pacientovi potvrzení o platbě (včetně uvedení termínu předplaceného parkování), na základě kterého bezpečnostní pracovník (vrátnice) určí pacientovi parkovací místo. Parkovací místa pro pacienty jsou vyhrazena za budovou O tj. zásobovací ústředna. Tato služba je zpoplatněna. Pacient obdrží od pracovnice pokladny kromě účetního dokladu o zaplacení též potvrzení o úhradě a poučení, o nutnosti jeho umístění na viditelném místě v zaparkovaném vozidle.

Pro motorová vozidla jsou vyčleněna níže uvedená parkoviště. V závislosti na aktuálním stavu bezpečnostní pracovníci informují řidiče vjíždějících motorových vozidel o možnosti a způsobu parkování. Dále provádí kontrolu parkování. Zjistí-li nesprávné parkování

upozorní řidiče na nesprávné parkování informačním letáčkem, který umístí za stěrač vozidla.

Osobami vstupujícími do areálu nemocnice jsou zaměstnanci nemocnice, zaměstnanci smluvních partnerů, pacienti, návštěvníci, zákazníci provozoven (kosmetika, kadeřnictví, bufetu apod.), služební návštěvy apod. V době návštěv je pohyb osob bez omezení s ohledem na případný stav těchto osob. Osoby v podnapilém stavu či pod vlivem omamných nebo psychotropních látek nejsou do objektu vpuštěny. Vstup v mimopracovní době je osobní branou u vstupu (V1) po provedené identifikaci osoby.

Pro vstup do ordinací a provozoven na vstupním objektu S se užije vstupních dveří u informací. Návštěvám bude v mimopracovní době a v době mimo pravidelnou dobu návštěv umožněn vstup na základě odsouhlasení lékařem příslušného oddělení. V mimopracovní době mají povolen vstup zaměstnanci smluvních partnerů a nájemci prostor v areálu. Pacientům a zákazníkům ordinací a provozoven umístěným na budově S bude vstup povolen jen po odsouhlasení příslušným ambulancním lékařem nebo provozovatelem provozovny. Totéž se týká i zákazníků kadeřnictví na budově A. Služební návštěvy (zástupci dodavatelských firem, osoby provádějící veřejnosprávní kontrolu, externí auditoři, exkurze, aj.) se pohybují v areálu a na pracovištích nemocnice vždy s vědomím vedoucího zaměstnance příslušného útvaru (nebo statutárního zástupce) a je-li to nutné nebo vhodné, v doprovodu pracovníka určeného vedoucím zaměstnancem příslušného útvaru. Služební návštěvy musí dbát zvláštního režimu jednotlivých pracovišť (např. pracoviště intenzivní péče, infekční oddělení, operační sály, sklady materiálů, plynů, aj.) v souladu s příslušnými provozními řády a dalšími vnitřními předpisy. Zaměstnanci externích firem, které pro nemocnici zajišťují dodávky služeb (např. stavení práce, servis a údržba technických zařízení,...), musí být prokazatelně seznámeni s riziky BOZP a PO pracovišť, na kterých budou dodávky zajišťovat. Seznámení provádí osoba odpovědná za zajištění dodávek ve spolupráci s vedoucím oddělení na kterém se dodávka nebo služba zajišťuje. Služební návštěvy po pracovní době jsou povoleny pouze v případech předem nahlášených nebo potvrzených vedoucím pracoviště. V mimopracovní době mají povolen vstup zaměstnanci nemocnice pracující v nepřetržitých provozech nebo pracovníci profesí, u kterých se vzhledem k jejich pracovnímu zařazení pohyb v areálu předpokládá. Pro vstup používají zaměstnanci osobní bránu u hlavního vstupu (V1). Zaměstnanci, kteří mají čipy od parkoviště pro zaměstnance používají pro vstup branku z parkoviště zaměstnanců.

Bránu (V2) dálkově ovládají bezpečnostní pracovníci. Je otevřena vždy jen na dobu nezbytně nutnou pro vjezd nebo výjezd. Hlavní vjezd tedy otevírání závory a branky u závory provádí bezpečnostní pracovníci. V případě nepřítomnosti ovládají závoru pracovníci informací. V případě nahlášeného vjezdu nebo výjezdu vozu ZZS JmK je závora zvedána v předstihu. Pokud vůz ZZS JmK zajíždí do objektu centrálního příjmu otevírají se v předstihu i vrata prostoru stanoviště vozů ZZS JmK. Branka u závory je otevřena v pracovní době a v době návštěv. V jinou dobu je vstup brankou možný jen po dohodě s bezpečnostním pracovníkem. Bezpečnostní pracovníci podávají potřebné informace vstupujícím nebo vjíždějícím. Pokud nejsou schopni informace poskytnout, odkážou žadatele o informace na pracovníci informací ve vstupním objektu. Branku ovládají zaměstnanci vstupující z parkoviště pro zaměstnance pomocí čipu, nebo na požádání bezpečnostní pracovníci. Bezpečnostní pracovníci průběžně kontrolují, zda branka není otevřená.

Klíčový režim Nemocnice Břeclav, příspěvkové organizace zajišťuje v potřebném rozsahu dostupnost všech prostor pro případ havarijních stavů, požáru nebo mimořádných událostí a dále minimalizuje riziko použití nebo zcizení klíčů neoprávněnými osobami. Areál nemocnice je rozdělen dle účelu na zóny poskytování zdravotní péče, technické prostory, společné prostory, prostory pronajatým právnickým a fyzickým osobám a ubytovnu pro zaměstnance. Odpovědným pracovníkem je zajištěno, aby klíče od svěřených prostor byly vždy v potřebném rozsahu dostupné jak pro běžné použití při plnění pracovních povinností k používání, tak pro případ havarijních stavů, požáru a mimořádných událostí. A aby na pracovištích byl stanoven režim pro zajištění minimalizace rizika zcizení nebo zneužití klíče neoprávněnými osobami. Na každém pracovišti je vyčleněno místo, kde jsou uloženy klíče od svěřených prostor. Rezervní klíč od místa uložení (určená místnost) je vždy uložen na informacích ve vstupním objektu nemocnice. Klíč musí být označen tak, aby bylo jednoznačně zřejmé, ve které místnosti jsou na příslušném odd. ostatní klíče uloženy. V případě, že dojde ke změně místa uložení klíčů na odd., je odpovědný pracovník povinen tuto změnu nahlásit na informace a zajistit výměnu rezervního klíče. Všechny klíče musí být řádně označeny (číslo dveří, název pracoviště, apod.). V případě, že jsou rezervní klíče od prostor pracoviště uloženy i na informacích, musí být všechny klíče označeny shodně. Odpovědný pracovník vede v potřebném rozsahu evidenci klíčů (označení klíče tj. číslo dveří, počet kusů, místa

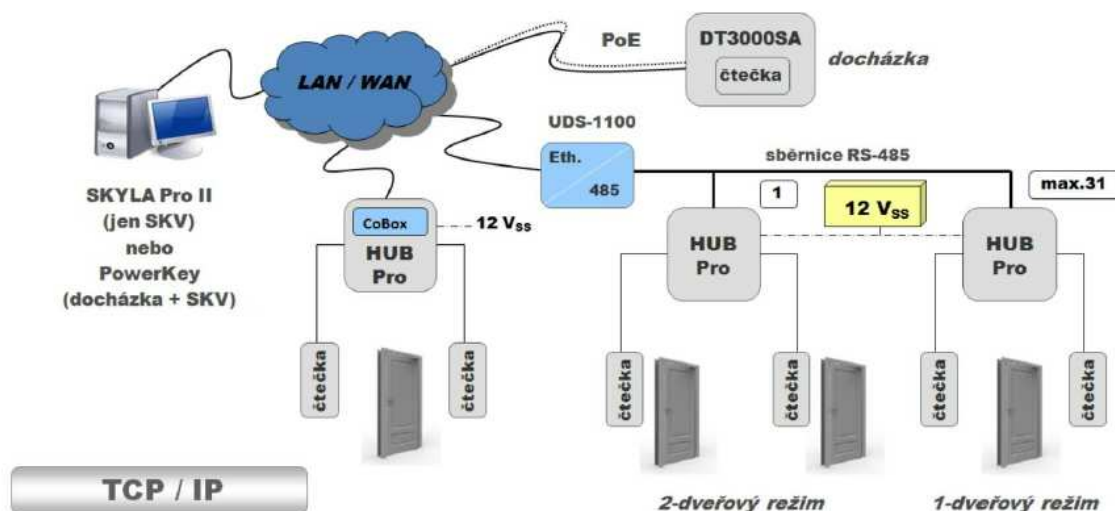


uložení rezervních klíčů, zapůjčení klíče např. pracovníkům servisních firem, atd.). Při ukončení pracovního poměru je zaměstnanec povinen přidělené klíče předat vedoucímu pracovníkovi oddělení. Zde je nutno dbát dodržování klíčového režimu a pravidelnou kontrolu všech vstupů pro ověření správnosti klíčů. Doporučuji uvést do směrnice nutnost periodických kontrol klíčů a zámků všech oddělení.

### 5.3 Elektronické systémy

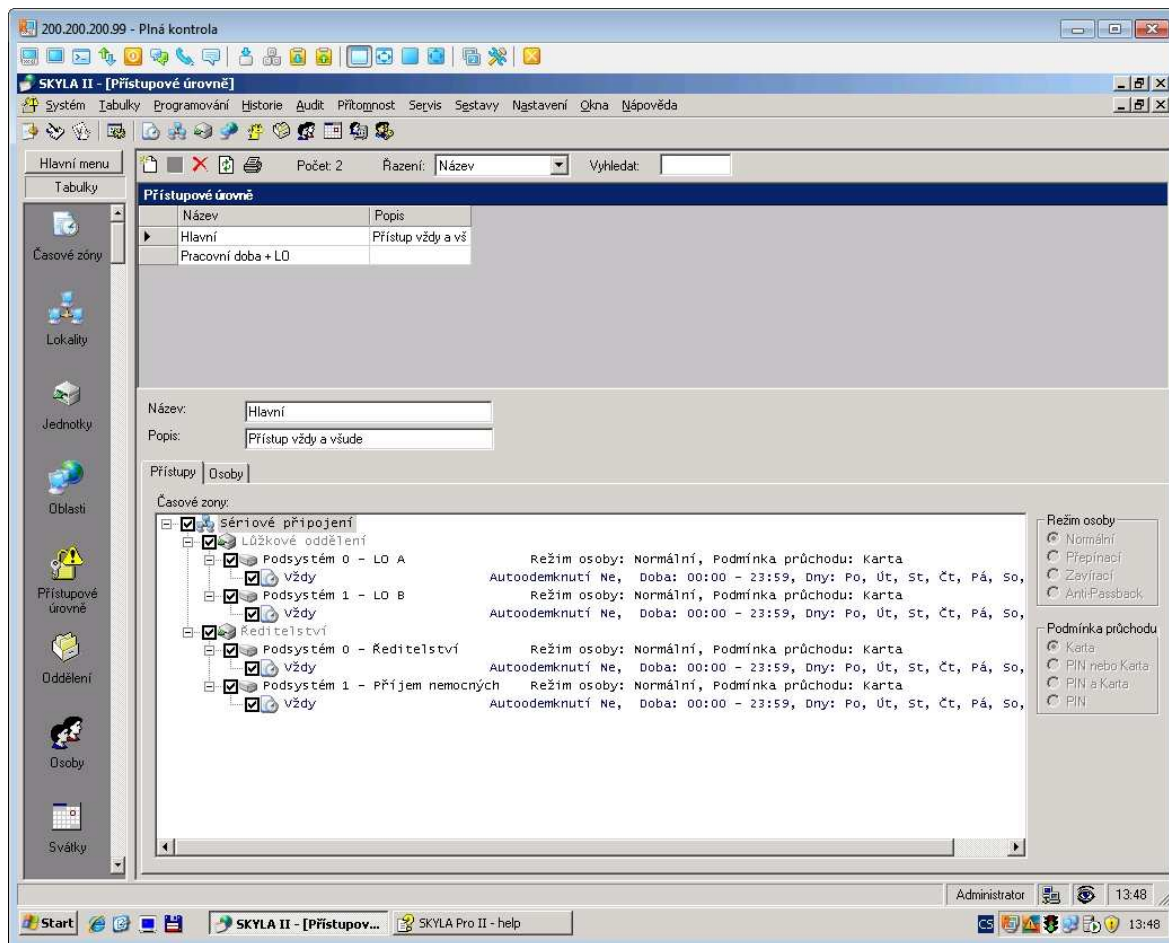
Jednotlivé budovy nemocnice jsou vybaveny elektrickou požární signalizací (dále jen EPS). Jednotlivé ústředny EPS jsou umístěny v místnostech s omezeným přístupem neoprávněných osob v 1.nadzemním podlaží budov. V lůžkových budovách jsou ústředny EPS umístěny v místnostech s nepřetržitým dohledem tj. na sesternách lůžkových oddělení umístěných v přízemích lůžkových budov. Hlavní ústředna PZTS je umístěna v místnosti Informací u hlavního vstupu do nemocnice, kde je personálem zajištěn nepřetržitý provoz a tím dohled nad provozem signalizačního zařízení.

Pro zabezpečení důležitých budov byl instalován **systém kontroly vstupu SKYLA Pro II** což je program pro konfiguraci, sběr dat a monitoring systémů kontroly vstupu malého až středně velkého rozsahu s řídicími jednotkami HUB Pro a docházkovými terminály DT2000 SA. Identifikační zařízení připojené na program umožňuje podrobné sledování jak vlastní činnosti přístupového systému (příchody, odchody, narušení režijních opatření apod.), tak i zpětné sledování a vyhodnocení operací a zásahů všech operátorů. Ze získaných dat může uživatel vytvářet filtrované přehledy, provádět základní vyhodnocení docházky nebo získaná data zpracovávat v docházkových programech DOCH32, příp. PowerKey. Jak popisuje obrázek č. 11 je možnost jednotlivé přístupové body (čtečky) rozmístit u vstupních dveří důležitých objektů a vzájemně je propojit do uceleného komplexu s centrální obsluhou a správou. O správu a aktuální programové vybavení by se staralo oddělení nemocniční informatiky a telekomunikací. Obsluha a kontrola by byla v kompetenci ostrahy objektu.



Obr. 11. Schéma zapojení systému kontroly vstupu Skyla Pro II [28]

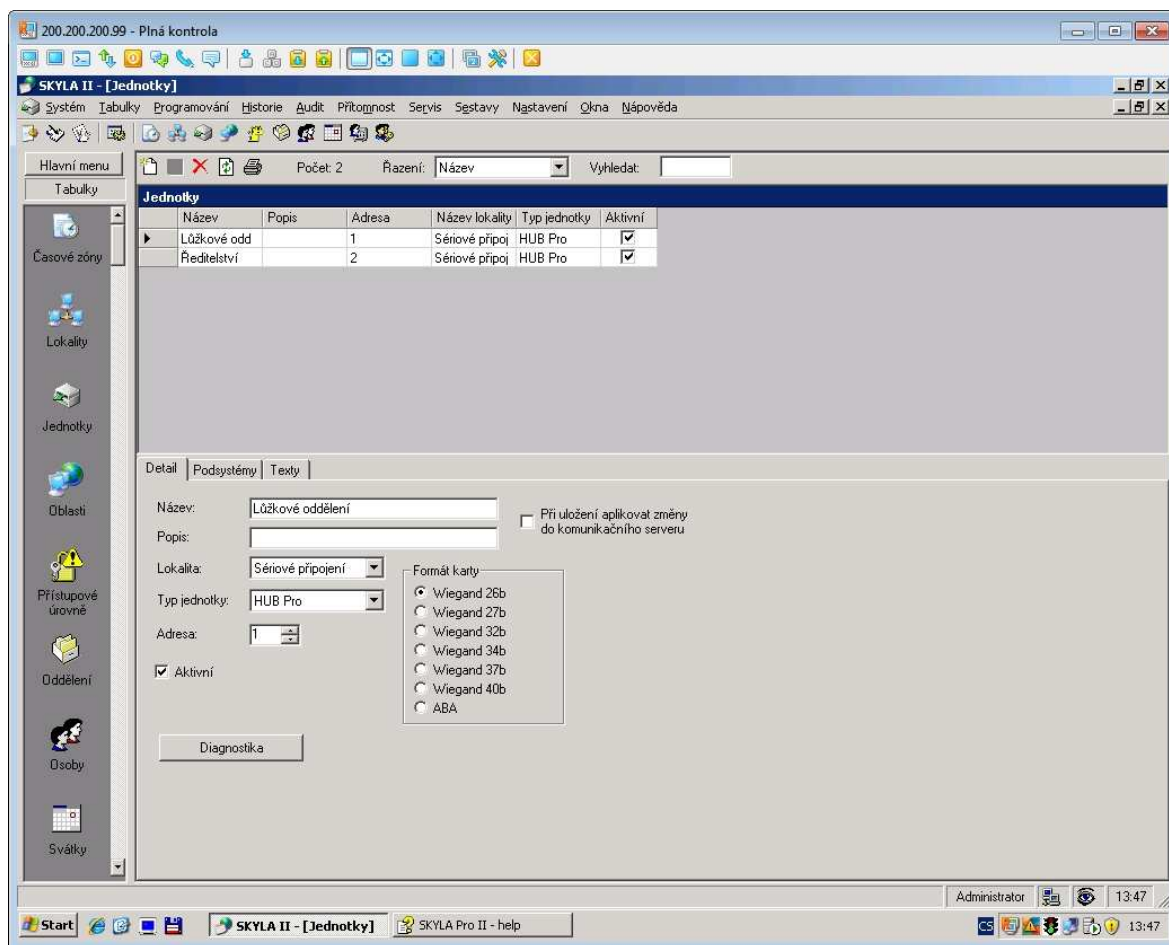
Aplikace SKYLA Pro II je určena pro operační systémy Windows 2000 Professional (Server) / XP Professional a je koncipována jako aplikace typu klient/server. Pro uživatele tento koncept přináší především možnost souběžné činnosti více operátorů. Jednotlivé klientské aplikace komunikují se serverem prostřednictvím TCP/IP protokolů – systém tak lze spravovat prakticky odkudkoliv. Přístup všech operátorů je chráněn heslem, administrátor může navíc každému z nich povolit přístup jen do některých částí programu. Heslem lze rovněž chránit přístup datového serveru k SQL databázím. Základní úlohou programu je nastavení přístupového systému. Jednoduchým a přehledným způsobem tak nadefinujete časové zóny, parametry všech jednotek HUB Pro i docházkových terminálů DT2000 SA, přístupové úrovně pro hromadné přidělování oprávnění kdo, kdy a kam může vstoupit, personální údaje osob včetně fotografií a uživatelsky nastavitelných poznámkových polí nebo oprávnění pro všechny operátory, kteří s programem mají pracovat.



Obr. 12. Nastavení přístupových úrovní

SKV SKYLA Pro II pracuje s přehlednou definicí přístupových práv pro osoby prostřednictvím přístupových úrovní. V každé této úrovni můžete kromě povolení nebo zakázání přístupu navíc i určit podmínku vstupu (pouze karta, pouze PIN nebo jejich kombinace) a také režim karty. Ten určuje, jak bude jednotka na platnou identifikaci osoby reagovat – prostým sepnutím relé na nastavenou dobu, jeho přepnutím do opačného stavu nebo rozepnutím, příp. zda bude aplikován tzv. režim anti-passback (kontrola směru průchodu). Přepínací režim slouží např. pro ovládání PZTS nebo zásuvkových okruhů. Dveře navíc mohou být díky funkci tzv. autoodemknutí odblokovány i zcela samočinně v předem určených časových oknech.

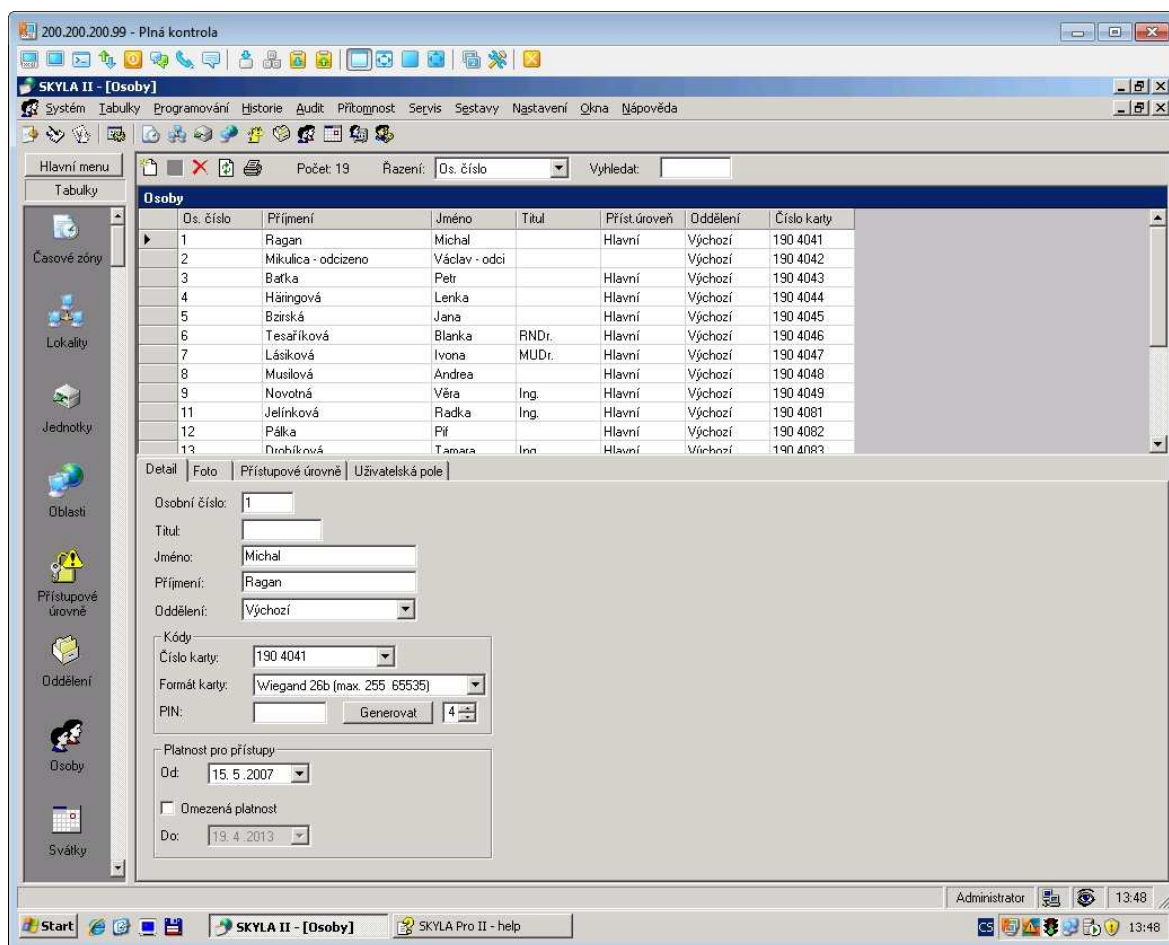
Monitorování systému provádí SKYLA Pro II dvěma způsoby: za prvé řádkovým způsobem vypisuje všechny události, které zaznamenávají jednotky HUB Pro nebo terminály DT2000 SA.



Obr. 13. Nastavení jednotek systému kontroly vstupu

Každá událost je doplněna o datum a čas vzniku a všechny ostatní potřebné informace (např. jméno a příjmení osoby). Tento přehled lze filtrovat, třídit a prohledávat podle různých kritérií nebo nechat program barevně odlišovat jednotlivé typy událostí ve výpisu.

Druhým způsobem sledování systému je záznam veškerých akcí operátorů – editace nebo mazání údajů v tabulkách, přihlášení, odhlášení apod. Komunikace s jednotkami HUB Pro nebo docházkovými terminály DT2000 SA může probíhat buď po metalické sběrnici RS-485 nebo dálkově přes LAN/WAN (TCP/IP) síť. Přímá podpora TCP/IP spojení umožňuje realizaci prakticky libovolně rozlehlého systému zahrnujícího např. i monitoring velmi vzdálených lokalit.



Obr. 14. Ukázka nastavení přístupových práv jednotlivých osob v systému

System je vybaven nástroji pro vytváření sestav. Jde o zpracované textové výpisy buď zaznamenaných událostí nebo obsahu databází. Výpis hledaných událostí lze filtrovat podle řady kritérií – data, času a místa vzniku, typu události nebo třeba jména osoby. Pomocí sestavy můžeme provádět i jednoduché vyhodnocení docházky (měsíční přehled přítomnosti, první a poslední událost za den apod.) nebo vytvořit přehled aktuální přítomnosti osob v objektu. Všechny tyto sestavy lze kromě vtištění i exportovat do souboru pro další zpracování.

Program umožňuje těsnou spolupráci s docházkovým programem DOCH v rámci systému Identita. Oba programy používají společnou databázi; záznam osoby provedený do tabulky SKYLY Pro II tak bude automaticky proveden i do databáze programu DOCH. Oba programy mohou využívat společný komunikační server, což umožňuje připojení jak

přístupových kontrolérů, tak i docházkových terminálů na společnou komunikační sběrnici a sjednocený sběr dat pro oba systémy.

Prostřednictvím programu SKYLA Pro II může operátor (zaměstnanec ostražky) v reálném čase i zjišťovat přítomnost osob v nadefinovaných zónách. Ty mohou být jak izolované, tak i vnořené. Vypsána je potom přítomnost každé osoby ve všech zónách, kde je přítomna – tedy aktuální i všech nadřazených. SKYLA Pro II nabízí celou řadu diagnostických nástrojů užitečných pro oživení systému nebo lokalizaci hardwarových problémů – od mapování sběrnic pro zjištění všech připojených a komunikujících jednotek až po podrobnou diagnostiku vybrané jednotky nebo docházkového terminálu. Tou můžete dálkově ověřovat stavy všech vstupů a výstupů, kontrolovat velikost napájecího napětí, mazat jednotlivé databáze v paměti jednotky nebo ovládat výstupy. Lze tak dálkově odemknout zámky, ovládat PZTS, rušit probíhající poplachy apod. SKYLA Pro II je vybavena sadou podpůrných nástrojů pro usnadnění a z pohodlnější práce obsluhy. Mezi ně patří např. automatické zálohování všech databází v nastavených intervalech, samočinné programování karet do pamětí jednotek pro bezobslužnou aktivaci a expiraci karet nebo posílání záznamů o probíhajících událostech na vybraný sériový port.

#### **5.4 Kamerové systémy**

Jednotlivé prvky stávajícího kamerového systému instalovaného v areálu nemocnice jsou nejednotné a jejich modernizace je neefektivní. Konzultoval jsem aktuální stav s vedoucím HTO a navrhli jsme modernizaci celého CCTV a po instalaci nových kamer následném sjednocení všech prvků jsou dovedeny do počítače v místnosti ostražky objektu a pomocí ovládacího programu instalovaném v počítači jsou jednotlivá místa pod kontrolou strážného konajícího ostražku. Na tento modernější CCTV je možno v budoucnu připojovat další kamery a takto systém rozšiřovat. Toto je zatím omezeno finanční dostupností dalších prvků.

Současný kamerový systém monitoruje pouze vybraná místa v areálu vycházející ne z konceptu, ale spíše z historického projektu. Nový kamerový systém musí splňovat moderní bezpečnostní požadavky a jednotlivé kamery by měly snímat nejen sledované území, ale kombinovaně i jiné kamery celého systému, aby tak byla zajištěna vzájemná kontrola jednotlivých kamer před sabotáží či zcizením.



Obr. 15. Kamerový systém v transportních chodbách

Kamerový systém instalovaný v transportních chodbách propojujících jednotlivé budovy v podzemí nemocnice slouží k ochraně majetku a kontrole pohybu neoprávněných osob. Připojení kamer v transportních chodbách k centrálním rozvodům je chráněno uzamykatelnou kovovou schránkou s poplachovým systémem, který je automaticky spuštěn při přerušení kontaktů z kamery nebo napájení. Tento poplachový systém vytvořil pracovník nemocnice, tedy není jeho schéma dostupné běžnými prostředky a eliminuje se tím jeho jednoduchá deaktivace. Stejně tak krádež kamer nebo částí kamerového vedení je signalizována tímto bezpečnostním prvkem. Kontrola stavu a funkčnosti záložní baterie je prováděna zpracovatelem zařízení v pravidelných cyklech. V době kontroly stavu baterie provádí i ověření funkčnosti celého zařízení.

O přítomnosti kamerového systému CCTV jsou informovány všechny osoby pomocí informativních štítků na vstupních dveřích jednotlivých budov.



Obr. 16. Ukázka informačních štítků o přítomnosti systému CCTV u vchodu

Povinnost ohlášení u Úřadu pro ochranu osobních údajů zajišťuje vedoucí HTO ve spolupráci s právním oddělením nemocnice. Sledována jsou veřejně přístupná místa jednotlivých budov a riziková místa v objektu nemocnice. O místech s instalovaným kamerovým systémem v případě změn jsou informováni zaměstnanci nemocnice v rámci interních sdělení a klienti nemocnice v rámci informačních materiálů.

Pacienti si uvědomují, že instalované kamerové systémy slouží k monitorování vybraných prostor a pořízený záznam může odhalit nebo pomoci odhalit případného pachatele přestupku nebo trestného činu. Vnímají tak přítomnost kamer jako součást zajištění jejich bezpečnosti v takovém zařízení, kterým je nemocnice.



## 5.5 Protipožární opatření

Za metodické řízení a kontrolu požární ochrany v zařízeních nemocnice odpovídá ředitel nemocnice. Metodické řízení a kontrola požární ochrany je nedílnou součástí jeho řídicí a kontrolní činnosti. V rámci hodnocení a jiné činnosti hodnotí také stav zajištění požární ochrany. Dle potřeby vyžaduje od vedoucích pracovníků pravidelné i mimořádné zprávy o stavu požární ochrany a na jejich základě pak činí potřebná opatření k odstranění zjištěných nedostatků. Ředitel nemocnice je povinen prostřednictvím technika požární ochrany a vedoucích technickohospodářských pracovníků zajistit stálý dohled nad dodržováním požárních předpisů a nařízení. Zejména provádění periodických preventivních prohlídek a označení činností se zvýšeným nebezpečím míst výstražnými tabulkami.

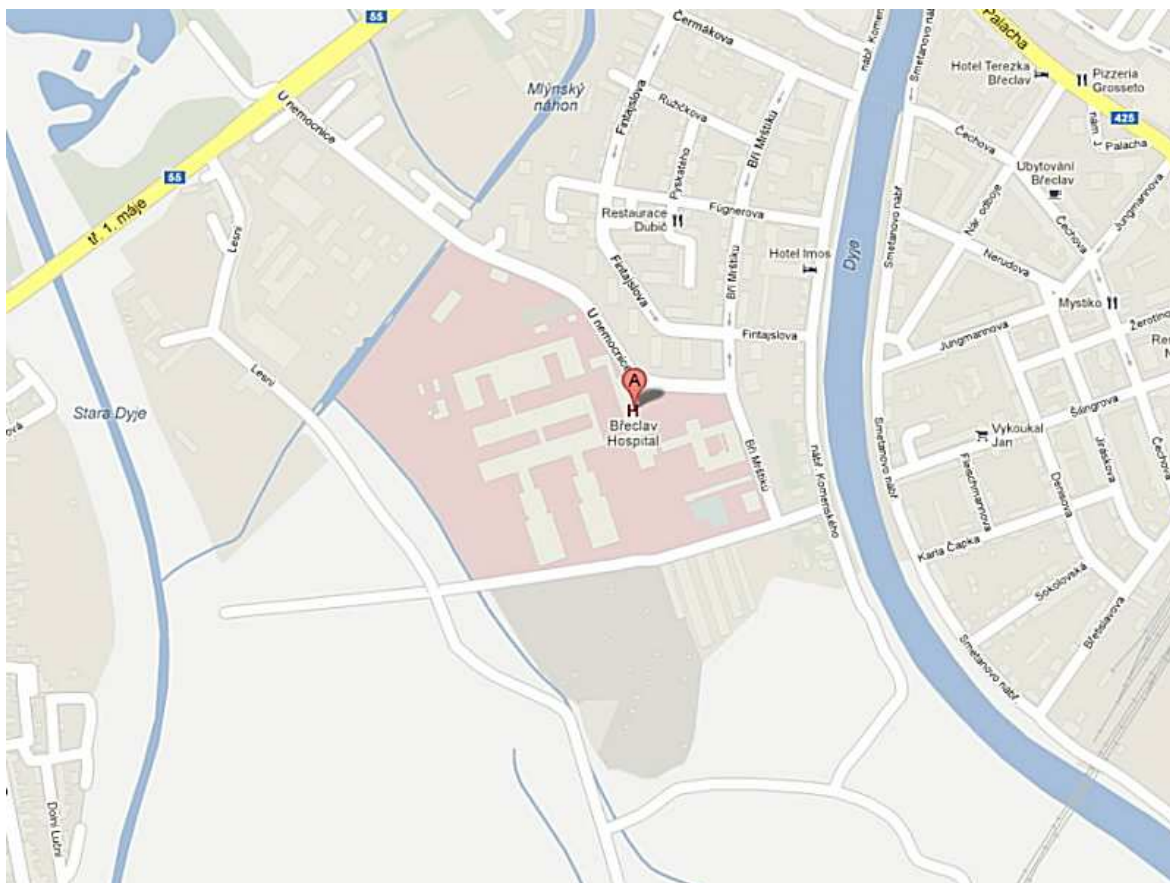
Za zajištění požární ochrany v objektu odpovídá vedoucí dle odpovědnosti stanovené Pracovním řádem organizace. Ostatní vedoucí pracovníci odpovídají za provádění protipožárních opatření a dodržování požárních předpisů na jimi řízených úsecích. Všichni zaměstnanci nemocnice jsou povinni dodržovat předpisy požární ochrany, plnit uložené úkoly na úseku požární prevence, účastnit se pravidelných školení a v případě potřeby se aktivně podílet na zdolávání požáru či evakuaci.

Pravidelně probíhá v rámci ověřování připravenosti složek IZS JmK cvičení se zásahem v nemocnici, kdy s pomocí studentů zdravotnické školy jako figurantů dochází k evakuaci vybraného oddělení a kontrole všech zabezpečovacích systémů. Ověřuje se tak i připravenost personálu a součinnost jednotlivých složek.

## 5.6 Přehled a hodnocení možných rizik

Mezi možná bezpečnostní rizika areálu nemocnice lze zařadit hrozby vnějšího i vnitřního nebezpečí. Do takových hrozeb lze zařadit požár, povodeň, výbuch zásobníku kapalného kyslíku, poškození elektroinstalace i elektrické požární signalizace, napadení, hrozbu nástražného výbušného systému a také v současné době možnost teroristického útoku. Dále je nutno brát na vědomí hrozbu fyzického napadení klientů nebo personálu nemocnice, únik dat či utajovaných skutečností nebo zdravotnické dokumentace, kontaminaci potravin či pitné vody nebo havárie inženýrských sítí.

Objekt nemocnice se nachází v blízkosti vodních toků a to ze dvou stran. Z toho důvodu je v případě hrozící povodňové vlny vedení nemocnice informováno o této skutečnosti v rámci krizového řízení JmK.



Obr. 17. Mapa umístění objektu nemocnice [19]

Nemocnice se nachází blízko toku řeky Dyje jak je patrné z obrázku č. 17, ale protipovodňové hráze zabezpečují hladinu proti vylití z koryta i v případě vyššího průtoku z vodní nádrže Nové mlýny, která se nachází přibližně 20 kilometrů proti proudu řeky. Po škodách způsobených posledními povodněmi v horním toku řeky Dyje byly provedeny důkladnější protipovodňová opatření po obou stranách hlavního koryta řeky v blízkosti města Břeclavi.

### Způsob identifikace a hodnocení rizik

Míra rizika (R) je stanovena individuálním ohodnocením vnímání rizika – rámcově vyjádření vnímaného dopadu (D) x pravděpodobnost výskytu (P); tj.  $R = D \times P$

### Identifikace potenciálních rizik na úrovni organizace

**VR – vnější rizika** – mimořádné události s hromadným postižením zdraví – hromadná neštěstí (HN), živelné katastrofy, průmyslové havárie, teroristické útoky, epidemiologická ohrožení,.... - nezpůsobená zaměstnanci ani procesy v organizaci, minimální vliv organizace a zaměstnanců na jejich zvládnání, nutná spolupráce s ostatními složkami IZS a zřizovatelem.

**PR – provozní rizika** - vyplývající z havarijních stavů – poruchy, přerušení dodávek energií, omezených kapacit zdrojů jak materiálních tak i personálních, nastavených standardních procesů, postupů - zvládaná přijetím opatření k jejich minimalizaci nebo vyloučení, zajištění náhradních zdrojů, zabezpečení personálu, změna organizace práce, technické dovybavení,

Tab. 1. Tabulka hodnot vybraných rizik

D – vnímaný dopad	P – pravděpodobnost výskytu rizika	R – míra rizika
0 – zvládaný	1 – téměř nemožná	<b>25 – 16 vysoká úroveň rizik</b> nutno řešit v rámci vrcholového vedení organizace – potřeba strategického rozhodování, zajištění finančních zdrojů,...., spolupráce s ostatními složkami IZS JMK, zřizovatelem – KU JMK
1 – téměř neznatelný	2 – výjimečně možná	
2 - drobný	3 – běžně možná	<b>15 – 9 střední úroveň rizik</b> řešení na úrovni vedení nemocnice, útvaru, oddělení, přijetí organizačních opatření, úprava pracovních postupů, postup dle havarijních, požárních a evakuačních plánů
3 – významný	4 – pravděpodobná	
4 – velmi významný	5 – hraničící s jistotou	<b>8 – 0 nízká úroveň rizik</b> - rizika přijatelná, řešitelná v rámci běžných opatření, řízení provozu - rizika, jejichž výskyt je nepravděpodobný, případnelze ovlivnit ze strany organizace, nutná spolupráce s ostatními složkami IZS, KU JMK
5 – nepřijatelný		

Tab. 2. Vybraná rizika dle bezpečnostní analýzy

<b>Vnější rizika</b>	<b>D</b>	<b>P</b>	<b>R</b>
Napadení fyzické ostrahy	3	3	4
Uložení NVS do budovy lůžkových oddělení	5	2	18
Uložení NVS do budovy zásobování	4	2	16
Uložení NVS do ostatních budov	3	2	15
Vandalismus	3	3	14
Napadení skupinou pachatelů (10-50 osob)	4	2	16
Teroristický útok	4	2	20
<b>Vnitřní rizika</b>	<b>D</b>	<b>P</b>	<b>R</b>
Selhání fyzické ostrahy	2	3	4
Výpadek funkce EPS	4	2	6
Výpadek funkce PZTS	5	2	8
Krádeže dokumentů a zdravotnické dokumentace	4	3	7
Použití biologické, radiologické či chemické látky	4	4	15
Únik zdravotnických a bezpečnostních dat	4	4	15

Z tabulky č. 2 jsou patrna veškerá zjištěná bezpečnostní rizika z provedené analýzy popisovaného objektu s ohledem na zjištěné skutečnosti a současné poměry v České republice a bezpečnostní situací v celém světě. Hrozba teroristického útoku v jakékoliv podobě s možností ohrožení zdraví a života osob je samozřejmě bezpečnostní riziko nejvyššího významu a pomocí všech dostupných prostředků se musí organizace mu zabránit nebo minimalizovat.

Tab. 3. Vybraná rizika vedoucí k aktivaci Traumatologického plánu

Vnější rizika	D	P	R
Výbuch plynu - podzemní zásobník	4	1	4
Terorismus - 3. stupeň 50-200 osob	4	1	4
Fosfa - únik fosforu - 4. stupeň - více jak 200 osob	5	1	5
Havárie letadla - 3. stupeň 50 - 200 osob	5	1	5
Terorismus - 4. stupeň 200 osob	5	1	5
Havárie letadla - 1. stupeň max 10 osob	3	2	6
Terorismus - 1. stupeň max 10 osob	3	2	6
Únik čpavku - Zimní stadion - 3. stupeň 50 až 200 osob	4	2	8
Havárie letadla - 2. stupeň max 50 osob	4	2	8
Terorismus - 2. stupeň max 50 osob	4	2	8
Železniční neštěstí 2. stupeň max 50 osob	3	3	9
Požáry (aglomerace) - 2. stupeň max 50 osob	3	3	9
Dopravní nehody (D2) 1. stupeň max 10 osob	3	4	12
Dopravní nehody (D2) 2. stupeň max 50 osob	4	3	12
Železniční neštěstí 3. stupeň 50 - 200 osob	4	3	12
Vnitřní rizika	D	P	R
Výpadek dodávky plynu	2	2	4
Výpadek dodávky vody	4	2	8
Výpadek dodávky elektrické energie	5	2	10
Požár nemocnice	4	3	12
Chřipková onemocnění, epidemie - nedostatek personálu	4	4	16
Povodně, živelné pohromy	4	4	16

### Charakteristika typů postižení zdraví

1. úrazy (těžké, střední, lehké)
2. popáleniny
3. intoxikace
4. ozáření
5. infekce

Traumatologický plán nemocnice je aktivován ve čtyřech stupních s ohledem na charakter a rozsah hromadného neštěstí. Stupně aktivace jsou v souladu se stupni poplachu dle Vyhlášky č. 328/2001 Sb., o některých podrobnostech zabezpečení integrovaného záchranného systému, ve znění pozdějších předpisů.

**I. stupeň** vyhláší krajské operační středisko ZZS JMK (dále jen KOS) jestliže bylo postiženo na zdraví **maximálně 10** osob, z toho 1 až 3 osoby jsou zraněny těžce (např. havárie osobních vozidel apod.);

**II. stupeň** – vyhláší KOS v případě MU při níž došlo k postižení zdraví **maximálně 50 osob**;

**III. stupeň** - vyhláší KOS v případě MU s postižením zdraví **od 50 do 200 osob**;

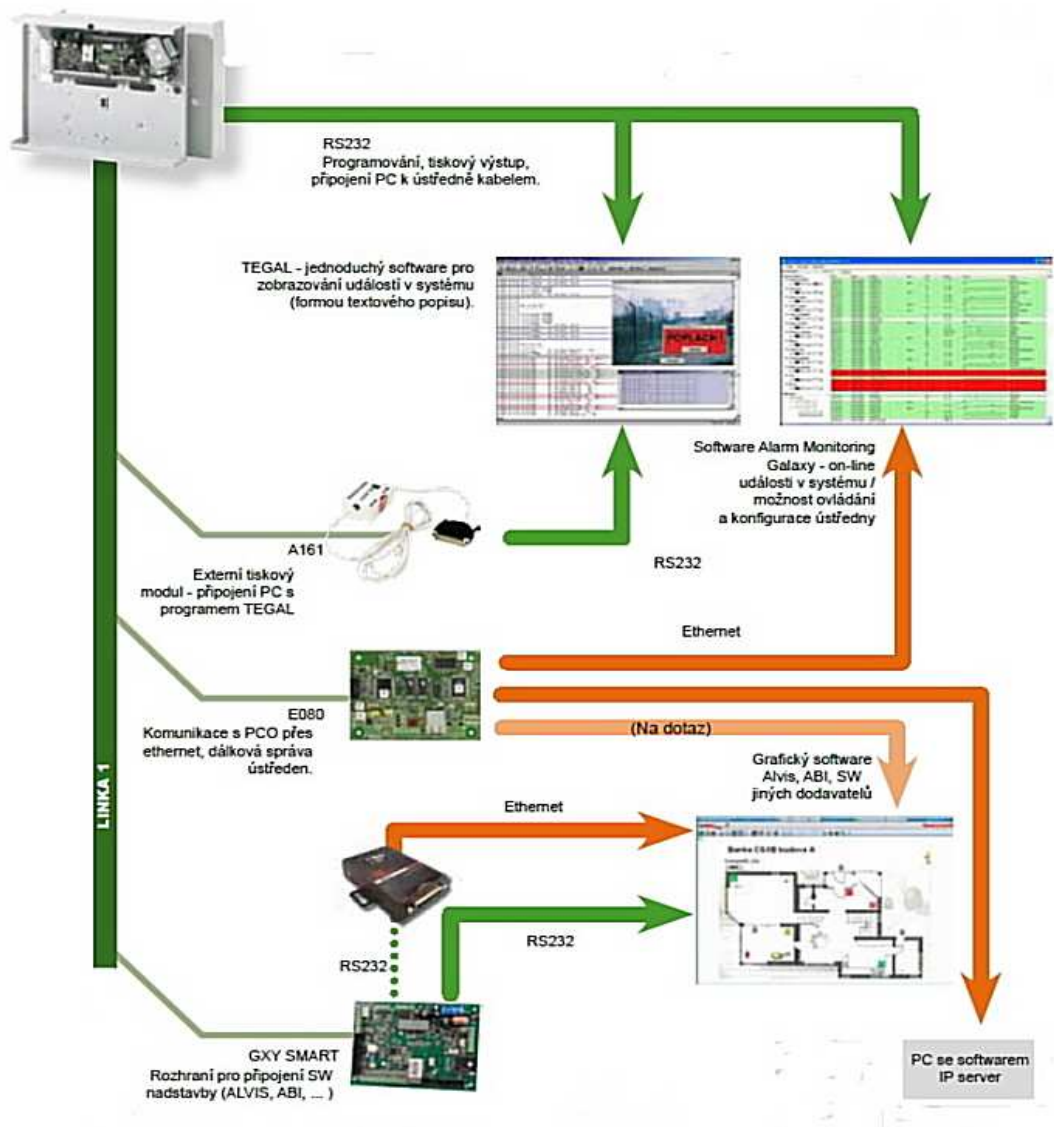
**IV. stupeň** (zvláštní) – vyhláší KOS v případě MU při postižení **více jak 200 osob**.

Traumatologický plán nemocnice navazuje na Traumatologický plán Jihomoravského kraje a ZZS JmK. Tímto plánem jsou koordinovány činnosti nezbytné k poskytování neodkladné zdravotní péče při hromadném neštěstí – mimořádné události s hromadným postižením zdraví, které je natolik rozsáhlé, že převyšuje běžnou kapacitu zdravotnického zařízení. Dále je v přiměřeném rozsahu aktivován v případě narušení provozních podmínek organizace z důvodu havarijních situací – havárií technických zařízení, omezení dodávek energií apod. Je to důležitá součást komplexního zabezpečení nemocnice, protože navazuje na situace hrozící při narušení bezpečnosti v objektu.

## 6 NÁVRH KOMPLEXNÍHO SYSTÉMU OCHRANY A BEZPEČNOSTI

Do priorit zabezpečení areálů zdravotnických zařízení je nutno zařadit bezpečí všech klientů a veškerého personálu v objektu. Dodržování zákonných předpisů a norem pro zajištění bezpečnosti. Opatření ochrany objektu musí umožnit eliminaci úsilí pachatele zmocnit se chráněného zájmu nebo jej nějak poškodit.

Ze zjištěných informací týkajících se současného stavu zabezpečení areálu nemocnice vyplývá, že je zapotřebí modernizovat jednotlivé prvky technické ochrany a vzájemně je integrovat. Modernizací a následnou integrací všech bezpečnostních systémů docílit propojení všech do ústředny PZTS.



Obr. 18. Návrh propojení jednotlivých součástí PZTS [28]

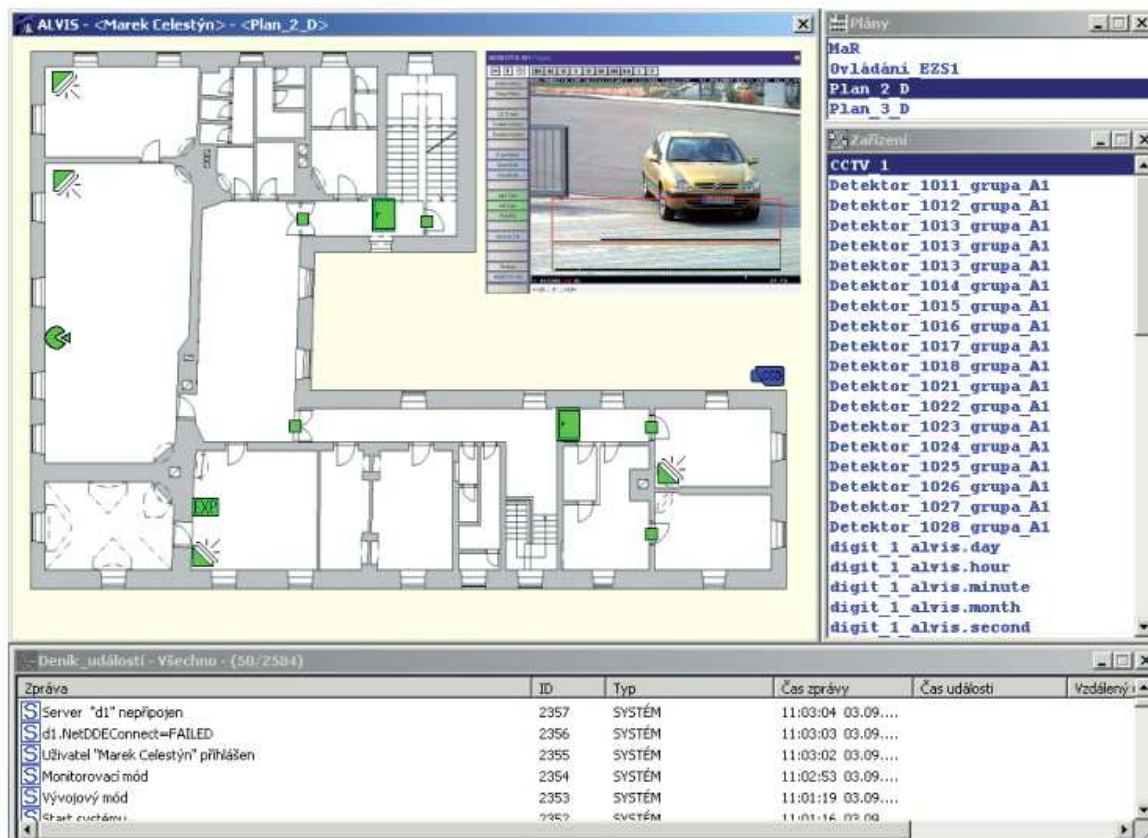
## 6.1 Návrh opatření ke snížení zjištěných rizik

Jedná se většinou o organizační opatření ke snížení rizik nebezpečí hrozícímu ve vztahu k objektům, pacientům nebo zaměstnancům nemocnice.

Jako hlavním bezpečnostním prvkem integrujícím instalované elektrické zabezpečovací systémy navrhuji instalaci ústředny PZTS s umístěním do místnosti ostrahy objektu s nepřetržitou službou. S ohledem na již instalované systémy EPS a SKV doporučuji instalaci ústředny Galaxy Dimension 520, která umožňuje integraci těchto elektronických systémů a navíc monitoring objektu a událostí pomocí univerzálního grafického prostředí Alvis. Komunikace mezi ústřednou a jednotlivými moduly systému probíhá po komunikační sběrnici RS485. Kabeláž systému musí být provedena tak, aby byly všechny moduly připojeny ke sběrnici paralelně.

**Univerzální grafické vývojové prostředí** Alvis je určené na tvorbu aplikací monitorovacích a řídicích systémů. Je vhodný všude tam, kde vzhledem k požadavkům obsluhy, složitosti sledovaného objektu, množství různých zařízení a prioritních úrovní, není možné bez použití počítačového systému dosáhnout přehledný flexibilní lehce adaptovatelný monitorovací, řídicí a výstražný systém. Alvis je založený na architektuře klient/server, což umožňuje distribuované rozdělení monitorovacího a výstražného systému na více počítačích, vzájemně propojených pomocí počítačové sítě LAN, WAN případně internet. Samotný program Alvis je klientem určeným na vizualizaci stavu monitorovaného prostoru. Pro svoji činnost využívá služby programových serverů, které komunikují s připojenými zařízeními a poskytují potřebné údaje. Neomezené množství programových serverů a klientů může být aktivováno v rámci počítačové sítě a na komunikaci mezi nimi se využívá standardní protokol DDE/NetDDE. Každý klient může zobrazovat libovolnou podmnožinu údajů poskytovaných dostupnými servery. Pro zabezpečení vlastního aplikačního souboru Alvisu je dostupná funkce uložení aplikace s uživatelsky definovaným heslem. Dále je možné chránit i vlastní grafické podklady pomocí hesla nebo elektronického digitálního podpisu. Soubory protokolu programu Alvis jsou kryptovány pomocí 128 bitového kryptovacího klíče. Všechny významné zásahy do programu Alvis jsou chráněny proti neoprávněné manipulaci. Systém hesel a přístupových práv umožňuje flexibilní nastavení oprávnění na vykonávání různých funkcí nezávisle pro jednotlivé pracovníky obsluhy (strážní služby).





Obr. 19. Ukázka použití univerzálního grafického prostředí Alvis [28]

Program podporuje připojování vzdálených zařízení pomocí modulů terminálových serverů (převodníků RS 232, TCT/IP). Tím umožňuje bezpečnostní monitoring vzdálených objektů a lokalit. Ve vývojovém režimu (chráněném superheslem) je možné definovat seznam operátorů, počet a druh informačních oken na obrazovce, parametry zobrazovaných oken (např. zda může obsluha změnit velikost oken a jejich umístění na obrazovce). Po přepnutí do režimu monitorování je možné vykonávat jen ty operace, na které má momentálně přihlášený operátor oprávnění. Komunikace mezi programovými moduly v počítačové síti je chráněná kryptovacím mechanismem tak, aby nemohla být zneužitá. V případě, že monitorované zařízení změní stav a nastane poplach, Alvis může automaticky zobrazit plán, na kterém je umístěný symbol daného zařízení. Symbol změní svou barvu, respektive tvar podle stavu, který nastal, zároveň může blikat a vydávat zvukový signál. V přehledovém okně poplachů se zobrazí poplachová zpráva, na obrazovce se objeví okno s instrukcemi pro obsluhu a s podrobnějším popisem stavu zařízení. Do protokolu událostí se zapíše protokolová zpráva spolu s datem a časem.

**Systém kontroly vstupu** Skyla Pro umožňuje integraci s jiným programem pro jejich další vyhodnocení. Tuto integraci navrhuji se systémem CCTV a EPS do PZTS. A to pro případ požáru a následné evakuace osob. Operátor tak bude mít přehled o pohybu osob ve střežených budovách a může je pak rychleji informovat o případném nebezpečí či hrozbě. Instalaci vstupních jednotek SKV nutno provést u vstupů pro personál do budov lůžkových oddělení, do budov zásobování a vstupu personálu z parkoviště zaměstnanců. Instalace SKV byla provedena pouze u vstupních dveří do budovy ředitelství. Tato instalace po změně využití donedávna nevyužitých prostor na nynější multioborovou JIP je tak bezvýznamná. Tedy neplní původně plánovanou funkci. Je třeba úpravy vstupu do prostor ředitelství a obnovení kontrolovaného vstupu.



Obr. 20. Systém kontroly vstupu u vstupních dveří budovy ředitelství [28]

Pro zamezení volného pohybu osob na jednotlivá lůžková oddělení doporučuji osazení vhodných klik na vstupní dveře všech lůžkových oddělení, aby byl možný volný pouze odchod z těchto oddělení. Pro vstup je nutný klíč dle klíčového režimu platného v tomto objektu. Ke vstupu tak budou oprávněny pouze osoby poučené nebo návštěvy pacientů po vpuštění službu konajícím zdravotnickým personálem. Eliminují se tak nepovolené vstupy na oddělení a s tím spojené epidemiologická rizika či rizika zneužití zdravotnických dat či krádeže zdravotnických i osobních věcí a zároveň bude zachována možnost volného opuštění oddělení v případě mimořádné události.

Pro řádný výkon strážní služby navrhuji posílení nočních služeb na dva pracovníky, aby jeden mohl zajišťovat výkon běžné strážní služby u vjezdu do areálu a druhý mohl

nepravidelnými obchůzkami po areálu a v jednotlivých budovách kontrolovat bezpečnost personálu a pacientů na lůžkových odděleních a ověřovat uzamčení stanovených vstupů.

Centrální ovládací a dozorový pult doporučuji umístit v místnosti ostrahy nemocnice kde jsou dovedeny signály všech kamer a to jak těch vně tak i uvnitř budov. Strážný tak bude mít přehled o dění ve sledovaných místech a zároveň přehled o pohybu osob ve vytyčených objektech a nakonec také přehled o požárním zabezpečení.

Jednotlivé budovy nemocnice je nutno dovybavit kamerami centrálního kamerového systému. Ke stávajícím sledovaným místům je nutno přidat sledování hlavního vstupu a vjezdové brány, prostor vstupu brankou z parkoviště zaměstnanců, prostor vstupů do lůžkových budov a prostor vstupu do vodojemu v objektu nemocnice. Jako doplňkový ač opodstatněný ke sledování se jeví prostor vstupu do ubytovny zaměstnanců.

Dosud není sledován hlavní vstup ani vjezd do objektu kamerovým systémem. Není tak možná případná následná identifikace vjezdu či vstupu neoprávněných vozidel a osob. Dále bych do kamerového systému přidal sledování všech obvodových oplocení a volných prostor v areálu nemocnice. Na oplocení bych doporučil instalovat informační tabulky, že je objekt sledován kamerovým systémem, aby tak byl částečně eliminován pokus vniknutí narušitele do objektu.

Prostor vstupní branky z parkoviště zaměstnanců doposud není sledován kamerovým systémem, proto je zapotřebí správné nasměrování blízké kamery tak, aby byl pohyb osob monitorován a tím eliminováno bezpečnostní riziko neoprávněného vstupu.

Budova ředitelství je nyní organizačně rozdělena na tři různé úseky a to primárně kompletní složky ředitelství, prostor anatomicko-patologické laboratoře a nakonec oddělení multioborové jednotky intenzivní péče s nepřetržitým provozem. Je zapotřebí technicky pomocí systému kontroly vstupu oddělit zdravotnické oddělení od stávajících úseků ředitelství. Beru-li na vědomí, že v prosotrách ředitelství jsou dokumenty a doklady.

V centrálních i okrajových částech by měly být umístěny důležité prvky zobrazovací techniky jako jsou kamerové a poplašné systémy, aby bylo možné sledování takových prostor z hlediska zajištění bezpečnosti nebo zvukovým či světelným signálem dát na vědomí hrozbu. Tyto cesty spojují jednotlivé budovy a jsou tak snadným místem pro pohyb v rámci areálu a to bez možnosti normální vizuální kontroly ostrahou. Je tady v případě nekontrolovaného úseku kamerovým či podobným systémem velké riziko pohybu

neoprávněných osob, krádeže materiálu či přerušení rozvodů energií nebo medicíálních plynů a také skladování nebezpečných materiálů či nástražných výbušných systémů.

V případě umístění nástražného výbušného systému by došlo k významnému narušení jak rutinního provozu nemocnice, tak k poškození majetku a s velkou pravděpodobností také poškození na zdraví či dokonce ke smrtelným zraněním. Pro snížení takového rizika je zapotřebí se věnovat možnosti umístění takového nebezpečného předmětu v blízkosti areálu nebo v některé z budov. Veškerý nestandardní pohyb osob po areálu, podezřelé chování osob nebo skupin je nutno hlásit pracovníkům ostrahy nebo vedení nemocnice. Navrhuji zajištění pravidelné kontroly odpadkových košů, míst kde jsou umístěny lavičky, ale také okolí výtahů a evakuačních schodišť. Zde by se i v případě vyhlášení planého poplachu mohlo zdržovat větší množství osob.

## ZÁVĚR

Cílem diplomové práce bylo zjistit a popsat aktuální stav zabezpečení areálu nemocnice a určit rizika bezpečnosti v návaznosti na to navrhnout komplexní systém řízení ochrany a bezpečnosti objektu nemocnice.

V rámci diplomové práce jsem zanalyzoval nejpravděpodobnější hrozby v rámci bezpečnosti, které by mohla Nemocnice Břeclav očekávat. Zjistil jsem přehledy hlavních bezpečnostních systémů podílejících se na současném zabezpečení objektu a byly navrženy změny, které by měly vést k eliminaci hrozeb. Změny spočívají především ve zlepšení stávajících prvků fyzické ochrany a jejich vzájemné integraci, zvýšení ostrahy objektu a spolupráce členů ostrahy s jednotlivými odpovědnými osobami. Tyto změny vyplynuly ze skutečností, které nemusí být vždy známy veřejnosti a osobám navštěvujícím objekty nemocnic za účelem zdravotnické péče.

Přínosem mé diplomové práce pro praxi je, že z pohledu komplexního zabezpečení areálu byl žádoucí soulad všech částí a vytvoření bezpečnostního komplexu. Součástí komplexu jsou kamerové, přístupové, zabezpečovací systémy a ovládací prvky. Takto vytvořené řešení má mnoho zásadních výhod, jak po ekonomické, tak po řídicí stránce. Ostraha objektu bude zajištěna v nepřetržitém provozu dvěma členy ostrahy nemocnice a tím bude minimalizováno riziko nekontrolovaného vstupu do areálu organizace a zároveň zvýšena bezpečnost osob nacházejících se v objektu zdravotnického zařízení. Dozorové centrum umístěné v místnosti ostrahy bude modernizováno a zvýší se tak počet sledovaných míst v areálu a navíc se zvýší komfort obsluhy jednotlivých částí zabezpečovacího zařízení instalovaných v objektu.

Navržená opatření a zařízení ve všech ohledech zvýší ochranu a bezpečnost zařízení a osob v areálu Nemocnice Břeclav a tím je cíl diplomové práce splněn.

Věřím, že tato práce může být jak návodem pro určení slabých míst zabezpečení v nemocnicích podobného typu, tak i předmětem k zamyšlení jaká bezpečnost je v současné době ve zdravotnických zařízeních v naší zemi.

S ohledem na prohlášení k diplomové práci v souvislosti jejího zveřejnění po obhajobě neuvádím v práci informace, které by mohly být podnětem k protiprávnímu jednání nebo jeho navádění. Tedy neuvádím místa instalace kamer vně i uvnitř objektu, vnitřní plány budov ani podobná data či informace.

Na závěr lze konstatovat, že při použití odpovídajících technických bezpečnostních prvků je nutno pro zabezpečení areálu dále zkoumat další možné zdroje nebezpečí, analyzovat je a následně odstraňovat. V případě dostupnosti lepších zabezpečovacích systémů na trhu je třeba zvažovat modernizaci nebo doplnění stávajících systémů o využitelné systémy jiné.

## CONCLUSION

The aim of this thesis was to identify and describe the current status of the hospital complex security risks and identify security in relation to design a comprehensive system of protection and safety of hospital building.

The thesis I analyzed the most likely threats to the security, which could be expected Břeclav Hospital. I find the overview of the main safety systems involved in the current security of the building and the proposed changes, which should lead to the elimination of threats. The changes consist primarily to improve physical protection of existing elements and their mutual integration, high-security facility and cooperation of the guards with the individual responsible persons. These changes result from the fact that may not always be known to the public and persons attending hospital building for medical care.

Contribution of my work in practice is that from the perspective of a comprehensive security area was desirable harmony of all parts and a security complex. The site includes video surveillance, access control, security systems and controls. Thus formed solution has many key benefits, both economic and the control site. Security guard will ensure the continuous operation of two members of the security hospital and thus will minimize the risk of uncontrolled entrance of the organization while increasing safety of persons in the building of medical facilities. Surveillance Center, located in room surveillance systems will be upgraded and will increase the number of monitored sites in the area and also to increase the comfort of individual parts of the signaling equipment installed in the building.

Proposed measures and in all respects will increase the protection and safety of persons and equipment in the hospital Breclav and the aim of the thesis is completed.

I believe that this work can be both a guide for determining security vulnerabilities in hospitals of similar type, and subject to ponder what security is currently in medical institutions in our country.

With regard to the thesis statement in the context of its publication after the defense does not mention the work information that could be subject to infringement or guidance. Then do not mention the place of installation of cameras inside and outside the building, inside building plans or similar data or information.

In conclusion we can say that the use of appropriate technical security features needed to secure the area further investigate other possible sources of danger, analyze and dispose of. In case of availability of better security systems on the market it is necessary to consider upgrading or supplementing existing systems on available systems other.



**SEZNAM POUŽITÉ LITERATURY**

- [1] LAUCKÝ, Vladimír. *Technologie komerční bezpečnosti I*. Vyd. 2. Zlín: Univerzita Tomáše Bati, 2004. 64 s. Učební texty vysokých škol. ISBN 80-7318-194-0.
- [2] LUKÁŠ, Luděk a kol. *Bezpečnostní technologie, systémy a management I*. 1. vyd. Zlín: VeRBuM, 2011. 316 s. ISBN 978-80-87500-05-7.
- [3] MERNA, Tony a AL-THANI, Fasal F. *Risk management: řízení rizika ve firmě*. Vyd. 1. Brno: Computer Press, 2007. 194 s. ISBN 978-80-251-1547-3.
- [4] GARCIA, M. L.. *The design and evaluation of physical protection systems*. 2nd ed. Boston: Elsevier/Butterworth-Heinemann, c2008. 351 p. ISBN 07-506-8352-X.
- [5] HOFREITER, L., LOVEČEK, T., VEĽAS, A. *Zásady a principy analýzy rizík v oblasti fyzickej a objektovej bezpečnosti*. Žilinská univerzita v Žilíně, Fakulta špeciálneho inžinierstva, Žilina, 2006.
- [6] NOŽINA, M. *Mezinárodní organizovaný zločin v České republice*. 1. vyd. Praha: Themis, 2003. 407 s. ISBN 80-7312-018-6.
- [7] ŠKRLA, Petr a Magda ŠKRLOVÁ. *Řízení rizik ve zdravotnických zařízeních*. 1. vyd. Praha: Grada, 2008, 199 s. ISBN 978-802-4726-168.
- [8] NĚMEC, M. *Organizovaný zločin: Aktuální problémy organizované kriminality a boje proti ní*. 1. vyd. Praha: Naše vojsko, 1995. 219 s. ISBN 80-206-0472-3.
- [9] SOUŠKOVÁ, M.; SPIRIT M., *Pracovní právo: podle úpravy platné od r. 2007*, 1. vyd. Praha : Oeconomica, 2008. 231 s. ISBN 978-80-245-1379-9.
- [10] LOVEČEK, Tomáš. *Pasivní prvky ochrany jako součást bezpečnostního systému*. Magazín SECURITY, ročník XIV, číslo 76,2/2007, s. 26-30. ISSN 1210-8723.
- [11] UHLÁŘ, Jan. *Technická ochrana objektů. I.díl, Mechanické zábranné systémy II*. Vyd. 1. Praha: Vydavatelství PA ČR, 2004. 179 s. ISBN 80-7251-172-6.
- [12] LEŠINGROVÁ, R. *Člověk a výkonnost - cílevědomé plánování*. [Česko] : Roma, 2006. 78 s. ISBN 80-903808-0-8.
- [13] FORSYTH, P. *Jak motivovat lidi*. 1. vyd. Praha : Computer Press, 2000. 121 s. ISBN 80-7226-386-2.

- [14] NĚMEC, M. *Organizovaný zločin: Aktuální problémy organizované kriminality a boje proti ní*. 1. vyd. Praha: Naše vojsko, 1995. 219 s. ISBN 80-206-0472-3.
- [15] DVOŘÁK, D. *Řízení projektů: nejlepší praktiky s ukázkami v Microsoft Office*. 1. vyd. Brno : Computer Press, 2008. 244 s. ISBN 978-80-251-1885-6.
- [16] Frank L., *Bezpečnostní prostředí České republiky* [online]. 2003, [cit. 2011-10-01]. Dostupné z WWW:  
[<http://www.defenceandstrategy.eu/filemanager/files/file.php?file=6375>].
- [17] NEMOCNICE BŘECLAV, p. o. *Organizační řád*. Břeclav, 2011, 27 s. Ř - 01.
- [18] NEMOCNICE BŘECLAV, p. o. *Příručka integrovaného managementu (IMS) Nemocnice Břeclav, p. o.* Břeclav, 2012, 23 s. PIMS - 01.
- [19] MAPA: Nemocnice Břeclav. *Google Inc. Mapy Google* [online]. [cit. 2013-05-02]. Dostupné z: [http://maps.google.cz/maps?hl=cs&gs\\_rn=11&gs\\_ri=psy-ab&cp=12&gs\\_id=1a&xhr=t&bav=on.2,or.r\\_qf.&bvm=bv.45580626,d.Yms&biw=1497&bih=880&um=1&ie=UTF-8&q=nemocnice+b%C5%99eclav&fb=1&gl=cz&hq=nemocnice+b%C5%99eclav&hnear=nemocnice+b%C5%99eclav&cid=0,0,12134010337932701612&sa=X&ei=FCI4UcL1EoWNtAbauoCoAw&sqi=2&ved=0CIIsBEPwSMAA](http://maps.google.cz/maps?hl=cs&gs_rn=11&gs_ri=psy-ab&cp=12&gs_id=1a&xhr=t&bav=on.2,or.r_qf.&bvm=bv.45580626,d.Yms&biw=1497&bih=880&um=1&ie=UTF-8&q=nemocnice+b%C5%99eclav&fb=1&gl=cz&hq=nemocnice+b%C5%99eclav&hnear=nemocnice+b%C5%99eclav&cid=0,0,12134010337932701612&sa=X&ei=FCI4UcL1EoWNtAbauoCoAw&sqi=2&ved=0CIIsBEPwSMAA)
- [20] OHSAS 18001. *MBK Consulting, s.r.o.* [online]. 2008 [cit. 2012-06-11]. Dostupné z: <http://www.mbk.cz/ohsas-18001-1999-2007>
- [21] ISO 14001. *MBK Consulting, s.r.o.* [online]. 2008 [cit. 2012-06-11]. Dostupné z: <http://www.mbk.cz/iso-14001>
- [22] ISO 9001. *MBK Consulting, s.r.o.* [online]. 2008 [cit. 2012-06-11]. Dostupné z: <http://www.mbk.cz/iso-9001>
- [23] FYZICKÁ BEZPEČNOST. *Národní bezpečnostní úřad*. [online]. 2012. vyd. [cit. 2013-05-02]. Dostupné z: <http://www.nbu.cz/cs/ochrana-utajovanych-informaci/fyzicka-bezpecnost/informace/>
- [24] Zákon ze dne 8. ledna 2009 trestní zákoník, ve znění pozdějších změn a doplňků. *Sbírka zákonů, Česká republika*. 2009, Částka 11, 40, s 354 – 464. Dostupný na WWW: <<http://www.mvcr.cz/soubor/sb011-09-pdf.aspx>>.

- [25] LISTINA ZÁKLADNÍCH PRÁV A SVOBOD. *Poslanecká sněmovna Parlamentu České republiky*. [online]. 16. prosince 1992. [cit. 2013-05-02]. Dostupné z: <http://www.psp.cz/docs/laws/listina.html>
- [26] ČESKÁ TECHNICKÁ NORMA: Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – část 7: Pokyny pro aplikace. *Úřad pro technickou normalizaci, metrologii a státní zkušebnictví*. [online]. duben 2011. [cit. 2013-05-02]. Dostupné z: [http://csnonlinefirmy.unmz.cz/html\\_nahledy/33/87986/87986\\_nahled.htm](http://csnonlinefirmy.unmz.cz/html_nahledy/33/87986/87986_nahled.htm)
- [27] ZÁKLADNÍ BEZPEČNOSTNÍ POJMY A VZTAHY. *Ing. Světlana Krausová*. [online]. 2010 [cit. 2013-05-02]. Dostupné z: [http://www.krausova.eu/rs/index.php?cz\\_system-rizeni-bezpecnosti-informaci-isms-dle-iso-iec-27001,53](http://www.krausova.eu/rs/index.php?cz_system-rizeni-bezpecnosti-informaci-isms-dle-iso-iec-27001,53)
- [28] PROKOP, Ing. Petr. ADI GLOBAL DISTRIBUTION. [online]. [cit. 2013-05-06]. Dostupné z: <http://www.adiglobal.cz/iiWWW/cz/produkty110.nsf/wp/projektanti>
- [29] JURICA, Ing. Pavel. NEMOCNICE BŘECLAV, p. o. *Dokumentace zdolávání požáru: Operativní karta*. 5.3.2012. Břeclav, 2012.
- [30] T-SOFT, a. s. *TerEx* [počítačový program]. Ver. 3.0.8. Praha, 2009. *Software pro rychlý odhad následků průmyslových havárií, úniků nebezpečných látek, teroristických útoků a následků útoků chemickými, biologickými a jadernými zbraněmi*, 42 MB. Vyžaduje MS Windows 2000 a lepší.

**SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK**

ARO	Anesteziologicko-resuscitační oddělení	
Bc.	Bachelor	Bakalář – vysokoškolský titul
BOZP	Bezpečnost a ochrana zdraví při práci	
CCTV	Closed Circuit Television	Uzavřené televizní okruhy
CLC	CELENEC	Evropská komise pro normalizaci v elektrotechnice
ČR	Česká republika	
ČSN	Česká státní norma	
DDE	Dynamic Data Exchange	Dynamická výměna dat
EMS	Environment management system	
EN	Evropská norma	
EPS	Elektrická požární signalizace	
HSMS	Hazardous Substance Management System	Management bezpečnosti a ochrany zdraví při práci
HTO	Hospodářsko-technické oddělení	
HUB	Rozbočovač	
IP	Internet protocol	Protokol síťové vrstvy
ISO	International Organization for Standardization	Mezinárodní organizace pro tvorbu norem
IZS	Integrovaný záchranný systém	
JIP	Jednotka intenzivní péče	
JmK	Jihomoravský kraj	
LAN	Local Area Networks	Lokální počítačová síť
MS-OB	Montované skelety opláštění budov	
MV	Ministerstvo vnitra	

---

NU	Nežádoucí událost	
NVS	Nástražný výbušný systém	
OHSAS	Occupational Health and Safety Advisory Services	Systém řízení bezpečnosti a ochrany zdraví
p. o.	Příspěvková organizace	
PIN	Personal identity number	Osobní identifikační číslo
PO	Požární ochrana	
PÚ	Požární úsek	
PZTS	Poplachové zabezpečovací a tísňové systémy	
QMS	Quality Management System	Systém řízení kvality
RZ	Registrační značka	
Sb.	Sbírka	
SKV	Systém kontroly vstupu	
SQL	Stuctured Query Language	Standardizovaný dotazovací jazyk
TCP	Transmission Control Protocol	Primární transportní protokol
TS	Technical Specification	Technická specifikace
Vyhl.	Vyhláška	
WAN	Wide Area Network	Rozlehlá počítačová síť
ZZS	Zdravotnický záchranný systém	

## SEZNAM OBRÁZKŮ

- Obr. 1. Principy řízení rizik a základní postupy [17]
- Obr. 2. Základní bezpečnostní pojmy a vztahy [27]
- Obr. 3. Náčrt areálu Nemocnice Břeclav, p. o. [18]
- Obr. 4. Plán areálu nemocnice [29]
- Obr. 5. Ukázka účinku NVS uloženého v igelitové tašce [30]
- Obr. 6. Situační plán nemocnice s vyznačením rizikových míst
- Obr. 7. Pozemní zásobník kapalného kyslíku monitorován pomocí CCTV
- Obr. 8. Vstupní brána ze zaměstnaneckého parkoviště
- Obr. 9. Oplocení objektu nemocnice s instalovaným kamerovým systémem
- Obr. 10. Dohledové centrum ostražky nemocnice
- Obr. 11. Schéma zapojení systému kontroly vstupu Skyla Pro II [28]
- Obr. 12. Nastavení přístupových úrovní
- Obr. 13. Nastavení jednotek systému kontroly vstupu
- Obr. 14. Ukázka nastavení přístupových práv jednotlivých osob v systému
- Obr. 15. Kamerový systém v transportních chodbách
- Obr. 16. Ukázka informačních štítků o přítomnosti systému CCTV u vchodu
- Obr. 17. Mapa umístění objektu nemocnice [19]
- Obr. 18. Návrh propojení jednotlivých součástí PZTS [28]
- Obr. 19. Ukázka použití univerzálního grafického prostředí Alvis [28]
- Obr. 20. Systém kontroly vstupu u vstupních dveří budovy ředitelství [28]

## **SEZNAM TABULEK**

Tab. 1. Tabulka hodnot vybraných rizik

Tab. 2. Vybraná rizika dle bezpečnostní analýzy

Tab. 3. Vybraná rizika vedoucí k aktivaci Traumatologického plánu

## **SEZNAM PŘÍLOH**

**PŘÍLOHA P I: VYJÁDŘENÍ HASIČSKÉHO ZÁCHRANNÉHO SBORU**

**PŘÍLOHA P II: SITUAČNÍ PLÁN NEMOCNICE BŘECLAV**



# PŘÍLOHA P I: VYJÁDŘENÍ HASIČSKÉHO ZÁCHRANNÉHO SBORU



**Hasičský záchranný sbor  
Jihomoravského kraje  
Územní odbor Břeclav  
Smetanovo nábřeží 13  
690 02, Břeclav**

Břeclav 21. ledna 2013

Počet listů: 1

Přílohy: 2

**Nemocnice Břeclav, příspěvková organizace**  
U Nemocnice 3066/1  
690 74 Břeclav

## **Analýza rizik pro nemocnici Břeclav, p.o.**

*Vyřizuje: por. Bc. Kateřina Kondlerová, tel.: 950 615 142, e-mail: katerina.kondleroval@jmk.izscr.cz*

*Kontroloval: kpt. Mgr. Josef Formánek*

Na základě Vaší žádosti Vám zasíláme přehled nám známých zdrojů ohrožení nemocnice Břeclav, p.o.

## **Nemocnice Břeclav, p.o., U Nemocnice 3066/1, 690 74 Břeclav**

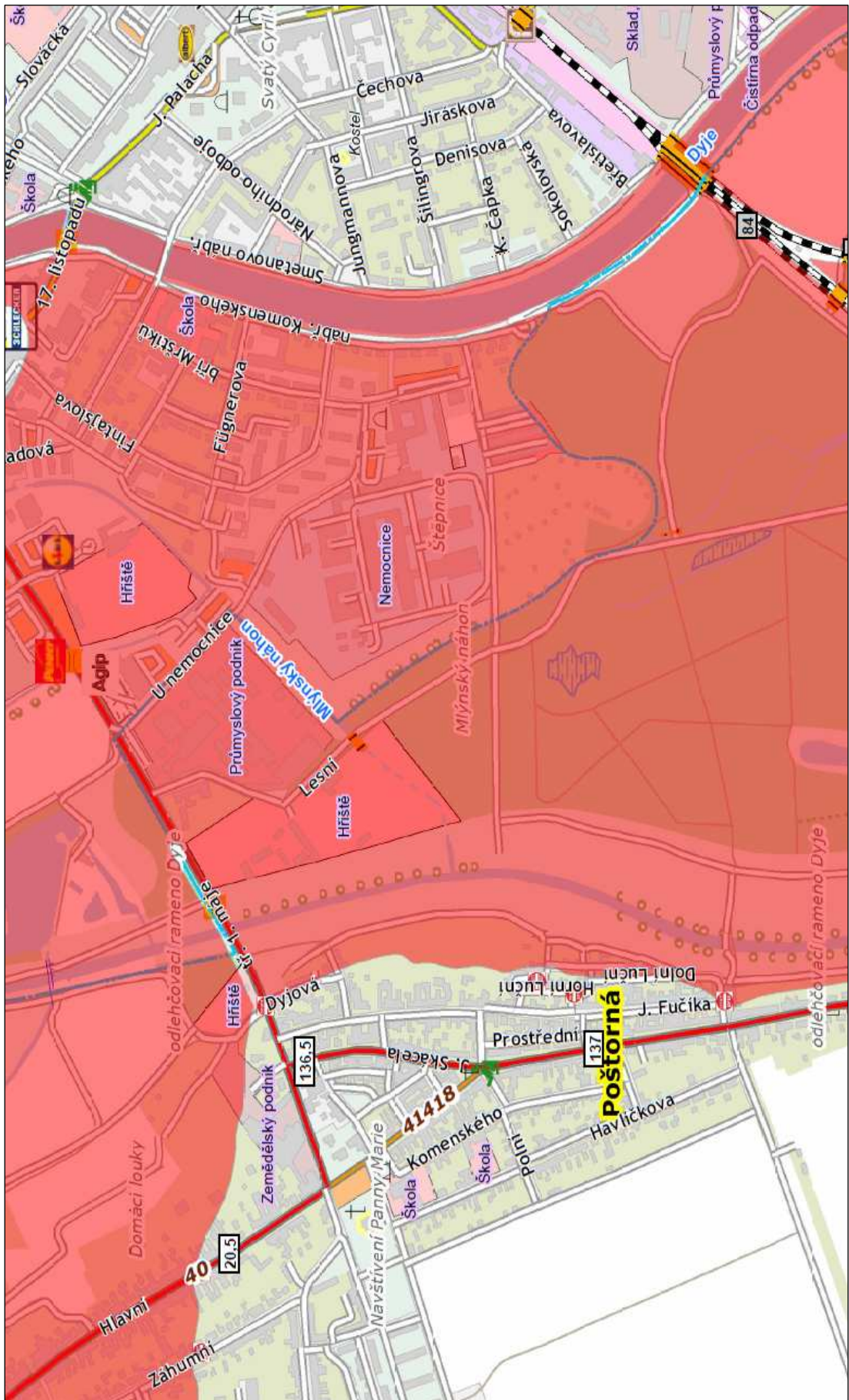
Nemocnice Břeclav, p.o., na adrese 690 74 Břeclav, U Nemocnice 1 je ohrožena:

- Přirozenou povodní (řeka Dyje) – (mapový podklad viz příloha č.1)
- Zvláštní povodní způsobenou narušením hráze VD Nové Mlýny. V případě ZPV1 způsobené porušením hráze VD Nové Mlýny dosáhne kulminace v zájmovém profilu 1318m3/s. Čelo vzestupné větve zvláštní povodně se nad Břeclaví objeví 14 minut před úplným porušením hráze. Kulminace povodňové vlny dorazí nad Břeclav za 17 hodin a 20 minut od začátku prolomení hráze, což znamená v čase za 13 hodin a 16 minut od úplného prolomení hráze. Hloubky vody v zaplaveném území dosáhnou až 3,5 m – (mapový podklad viz příloha 2)

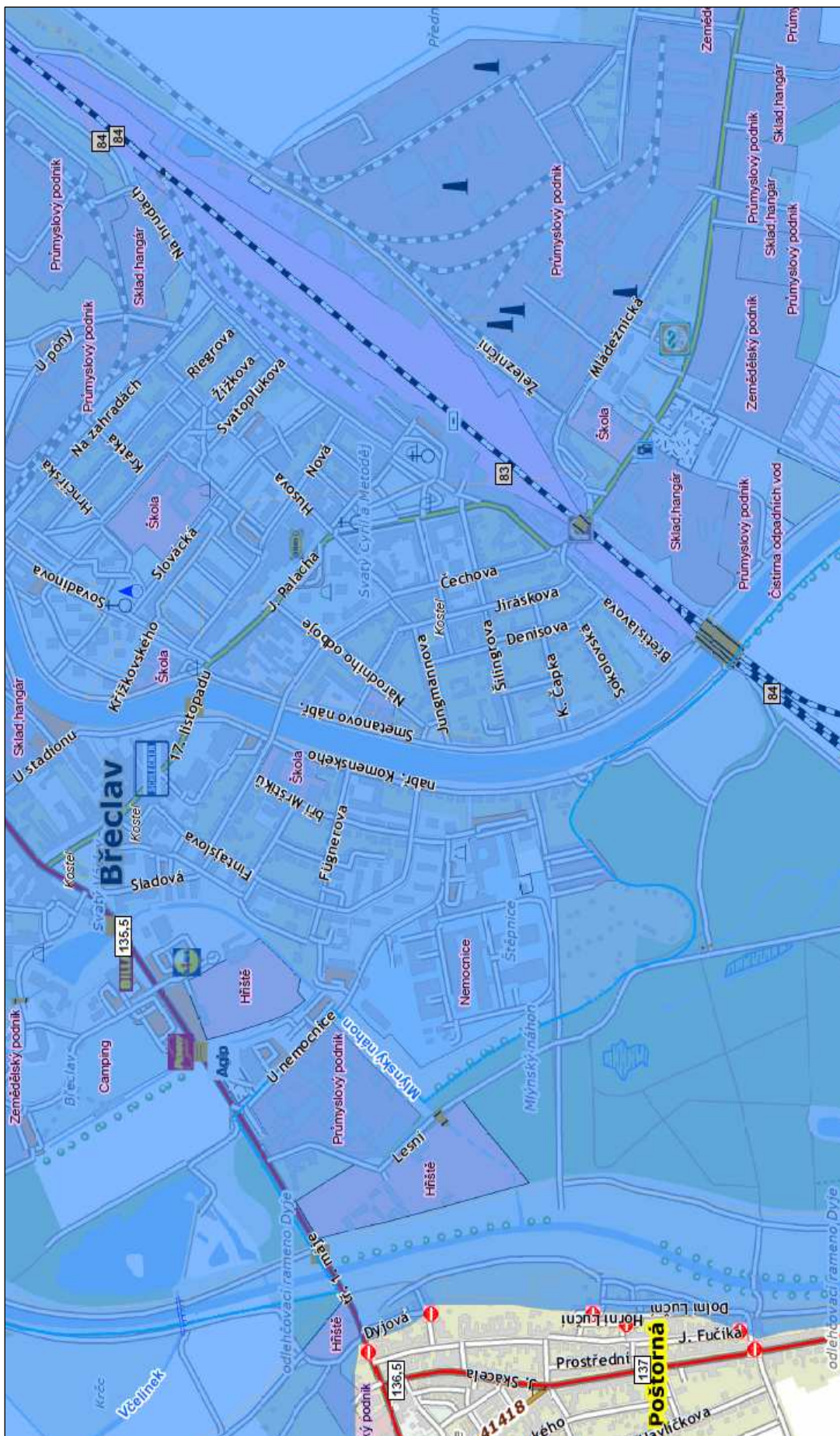
Pozn.: Bližší informace ke zvláštním povodním získáte na Povodí Moravy.

plk. Ing. František Hušek, Ph.D.  
ředitel územního odboru Břeclav  
Hasičského záchranného sboru  
Jihomoravského kraje

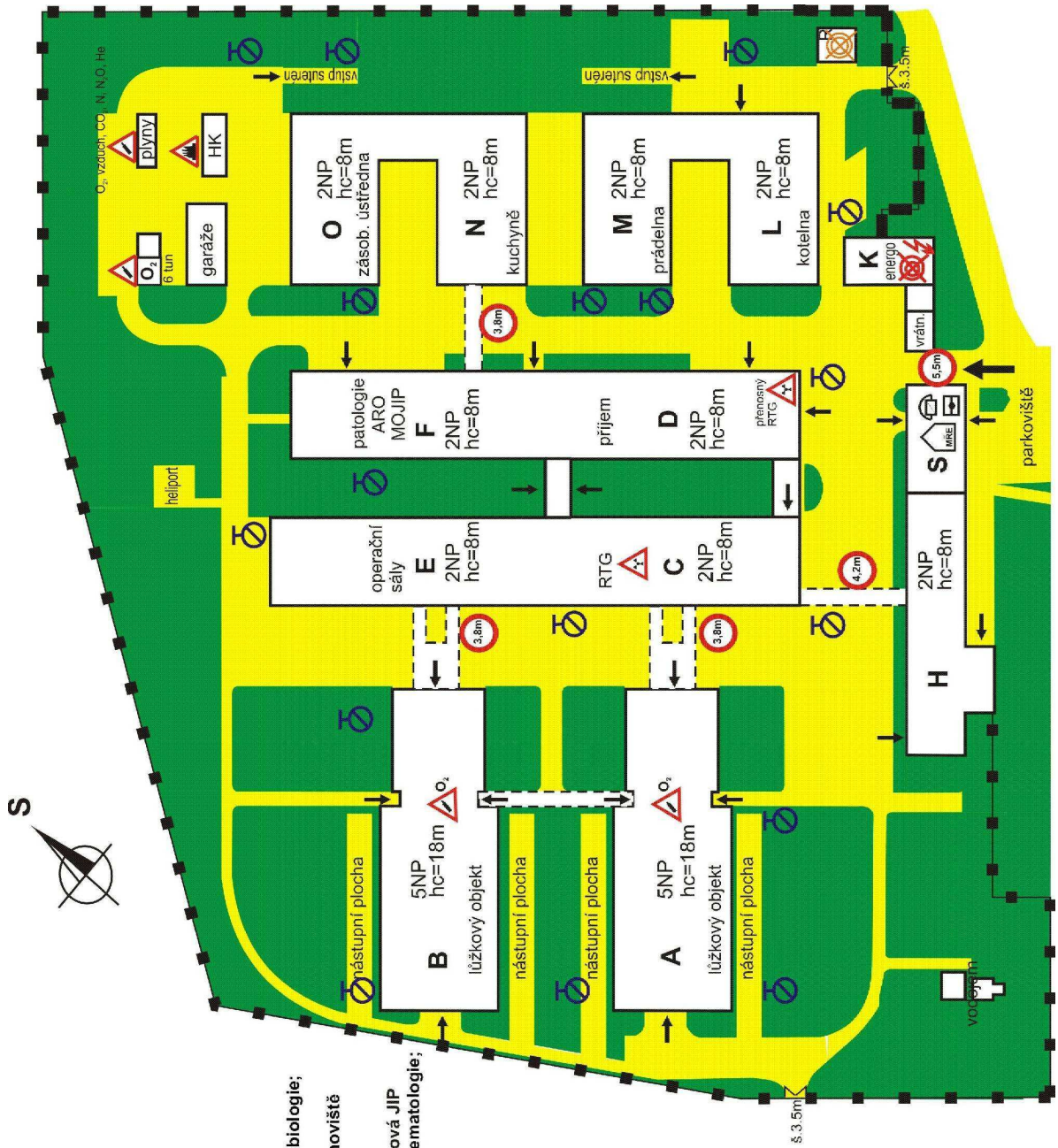
Příloha č. 1



Příloha č.2



# PŘÍLOHA P II: SITUAČNÍ PLÁN NEMOCNICE BŘECLAV



IMĚÍ: 1:500	Název: Nemocnice Břeclav p.o.
Schválil:	situace
	Změny
Dne: 03/2012	Provedl - podpis
	FIRE-STOP, Břeclav
	R. Ryšavý, OZO v. PO Z.525.98
MUDr. Janka Bambasová-ředitelka	<i>[Signature]</i>

- LEGENDA :**
- A – budova lůžkového objektu I.
  - B – budova lůžkového objektu II.
  - C – odd. laboratorní biochemie; odd. laboratorní mikrobiologie; radiodiagnostické odd.
  - D – fyziotricko-rehabilitační odd.; centrální příjem, stanoviště vozidel RZP
  - E – odd. ARO; odd. COS-CS
  - F – anatomicko-patologické odd.; ředitelství, mezioborová JIP
  - H – hematologicko- transfúzní odd.; odd. laboratorní hematologie; Remedia
  - S – lékárna; informace, vstup
  - L – plynová kotelna
  - M – prádelna
  - N – kuchyně
  - O – zásobovací ústředna
  - P – hospodářský dvůr
  - V – vrátnice, prodejna ovoce
  - T - trafostanice a náhradní zdroj (diesselagregát)
  - O<sub>2</sub> - odparovací stanice kyslíku
  - R - regulační stanice plynu