

# **Návrh a optimalizace zabezpečení nemocničního informačního systému AMIS\*H v Nemocnici Břeclav**

The Design and Optimization of Hospital Information System  
AMIS\*H Security at Hospital Breclav

Bc. Petr Bařka

---

Diplomová práce  
2013



Univerzita Tomáše Bati ve Zlíně  
Fakulta aplikované informatiky

---

Univerzita Tomáše Bati ve Zlíně  
Fakulta aplikované informatiky  
akademický rok: 2012/2013

## ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Bc. Petr Bařka**  
Osobní číslo: **A11364**  
Studijní program: **N3902 Inženýrská informatika**  
Studijní obor: **Bezpečnostní technologie, systémy a management**  
Forma studia: **kombinovaná**

Téma práce: **Návrh a optimalizace zabezpečení nemocničního  
informačního systému AMIS\*H v Nemocnici Břeclav**

Zásady pro vypracování:

1. Proveďte analýzu současné situace z pohledu řešeného problému.
2. Vypracujte návrh řízení vybraných bezpečnostních rizik ve vybraném informačním systému.
3. Navrhněte vhodnou implementaci zásad zabezpečení ve vztahu k vybraným bezpečnostním rizikům.
4. Aplikujte zásady v rámci vybraného informačního systému.
5. Analyzujte funkčnost vybraných zásad.

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **Bezpečnost informačních systémů, Petr Hanáček, Jan Staudek, 2000.**
2. **Příručka o ochraně dat pro veřejnou správu, 2005.**
3. **Závislost prosperity firmy na bezpečnosti informací, Roman Jašek, 2005.**
4. **Průvodce zabezpečením pro malé organizace, Donald Wilson, 2004.**
5. **Moderní počítačové viry, Igor Hák, 2005.**
6. **Lékařská informatika, Pavel Kasal, 1998.**

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 provozování, zabezpečení a návrhu na optimalizaci zabezpečení nemocničního informačního systému AMIS\*H v Nemocnici Břeclav. Dodavatelem tohoto informačního systému je firma ICZ a.s. a v Nemocnici Břeclav je provozován od roku 1994. Postupem doby byl systém několikrát upgradován a to jak po stránce hardwarové, tak po softwarové až do dnešní podoby, kdy je provozován na serveru HP Integrity rx2800 i2 4-jádrovým procesorem Intel Itanium 9320. Taktéž byla upgradována datová síť od propustnosti 10 Mbps HD po dnešní propustnost 1Gbps.

Klíčová slova: optimalizace, zabezpečení, nemocniční informační systém

## **ABSTRACT**

The thesis discusses the operation, security and design to optimize security hospital information system AMIS \* H Hospital Breclav. The supplier of the information system, the company ICZ as Břeclav Hospital and is operated since 1994. Over time the system has been upgraded several times and both the hardware and the software until today, when it is running on an HP Integrity rx2800 i2 4-core processor Intel Itanium 9320th It also has been upgraded data network throughput from 10 Mbps to today's HD 1Gbps throughput.

Keywords: optimization, security, hospital information system

Děkuji vedoucímu diplomové práce 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 20. 5. 2013

.....  
podpis diplomanta

**OBSAH**

<b>ÚVOD</b> .....	<b>9</b>
<b>I TEORETICKÁ ČÁST</b> .....	<b>10</b>
<b>1 NEMOCNIČNÍ INFORMAČNÍ SYSTÉMY</b> .....	<b>11</b>
1.1 LEGISLATIVA TÝKAJÍCÍ SE NEMOCNIČNÍCH INFORMAČNÍCH SYSTÉMŮ.....	11
1.2 VÝVOJ NEMOCNIČNÍCH INFORMAČNÍCH SYSTÉMŮ .....	17
1.3 INTEGRACE FIREM.....	18
1.3.1 ICZ, a. s. ....	19
1.3.2 Stapro, spol s r. o.....	19
1.3.3 CompuGroup Medical Česká republika, spol. s r. o. ....	20
1.4 NÁRODNÍ ZDRAVOTNÍ SYSTÉM .....	21
<b>2 OBECNÝ POPIS NEMOCNIČNÍHO INFORMAČNÍHO SYSTÉMU</b> .....	<b>23</b>
2.1 KLINICKÉ MODULY .....	23
2.1.1 Lůžkové oddělení .....	23
2.1.2 Ambulance .....	24
2.1.3 Laboratoře .....	25
2.1.4 Radiodiagnostické oddělení .....	26
2.2 ADMINISTRATIVNÍ MODULY.....	27
2.2.1 Pojišťovna .....	28
2.2.2 Účetnictví .....	28
2.3 PROVOZNÍ MODULY .....	29
2.3.1 Stravovací provoz.....	29
2.3.2 Dopravní zdravotní služba .....	30
2.4 SPRÁVA SYSTÉMU .....	31
<b>3 ZÁKLADNÍ DEFINICE TÝKAJÍCÍ SE BEZPEČNOSTI NEMOCNIČNÍCH INFORMAČNÍCH SYSTÉMŮ</b> .....	<b>32</b>
3.1 BEZPEČNOSTNÍ HROZBY NEMOCNIČNÍCH INFORMAČNÍCH SYSTÉMŮ .....	34
<b>II PRAKTICKÁ ČÁST</b> .....	<b>35</b>
<b>4 NEMOCNIČNÍ INFORMAČNÍ SYSTÉM AMIS*H</b> .....	<b>36</b>
4.1 UPGRADE CENTRÁLNÍHO SERVERU .....	38
4.2 UPGRADE DATOVÉ SÍTĚ .....	39
<b>5 SWOT ANALÝZA</b> .....	<b>40</b>
<b>6 NÁVRH A OPTIMALIZACE ZABEZPEČENÍ</b> .....	<b>43</b>
6.1 HARDWAROVÉ ZABEZPEČENÍ .....	43
6.1.1 Centrální prvek.....	45
6.1.2 Přístupové aktivní prvky .....	45
6.1.3 IP adresace.....	46
6.1.4 Uživatelská VLAN.....	46
6.1.5 TOP management a finanční oddělení .....	47

---

6.1.6	Správa nemocničního informačního systému.....	48
6.1.7	Management aktivních prvků.....	50
6.2	SOFTWAREVÉ ZABEZPEČENÍ.....	51
6.3	APLIKAČNÍ ZABEZPEČENÍ .....	53
6.3.1	Návrh a optimalizace aplikačního zabezpečení .....	56
<b>ZÁVĚR .....</b>		<b>61</b>
<b>ZÁVĚR V ANGLIČTINĚ.....</b>		<b>62</b>
<b>SEZNAM POUŽITÉ LITERATURY.....</b>		<b>63</b>
<b>SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK .....</b>		<b>65</b>
<b>SEZNAM OBRÁZKŮ .....</b>		<b>66</b>
<b>SEZNAM TABULEK A GRAFŮ.....</b>		<b>67</b>



## ÚVOD

Základní kámen Nemocnice Břeclav byl položen v roce 1986. Projekt byl však tvořen již podstatně dříve, v polovině sedmdesátých let a byl poplatný této době. Výstavba byla původně započata jako atypická bytová výstavba a teprve později došlo k oficiální změně projektu na nemocnici jako takovou. Výstavba byla plánována na dvě etapy. V roce 1992 byla uvedena do provozu 1. etapa - neoperační obory a vyšetřovací složky, 2. etapa - operační obory, ARO, centrální operační sály a centrální sterilizace byla uvedena do provozu v roce 1996. V současné době je Nemocnice Břeclav, p. o. jedním z nejvýznamnějších zaměstnavatelů v regionu, který svým významem pokrývá celý okres, částečně spádově přilehlé okresy, slovenské a rakouské příhraničí. Zaměstnává více jak 800 zaměstnanců, z čehož je zhruba 700 zdravotnických pracovníků v lékařských i nelékařských oborech, zajišťujících zdravotní péči, zahrnující nepřetržitý statimový a rutinní provoz oddělení a laboratoří včetně zajištění lékařské služby první pomoci. Zřizovatelem nemocnice je Jihomoravský kraj, jako vyšší samosprávný územně správní celek. Nemocnice Břeclav, p. o. je certifikovaná společností BUREAU VERITAS CERTIFICATION dle norem ČSN EN ISO 9001:2009, ČSN EN ISO 14001:2005 a ČSN EN OHSAS 18001:2008. V letošním roce probíhá akreditace laboratoří dle ČSN EN ISO 15189.

Ve své diplomové práci bych se chtěl zaměřit na návrh a optimalizaci zabezpečení provozovaného nemocničního informačního systému AMIS\*H a to na základě provedené SWOT analýzy, u které předpokládám, ve výskytu slabých stránek a hrozeb bezpečnostní rizika k řešení. Cílem práce je návrh a optimalizace zabezpečení na třech úrovních: hardwarové, softwarové a aplikační.

## **I. TEORETICKÁ ČÁST**

## 1 NEMOCNIČNÍ INFORMAČNÍ SYSTÉMY

Nemocniční informační systémy byly v České republice implementovány od začátku roku 1992, kdy jednou z prvních firem na českém trhu, která se zabývala implementací nemocničních informačních systémů byla firma SET, a. s.. Filozofie firem, které se zabývaly problematikou nemocničních informačních systémů byla bohužel na počátku devadesátých let chybná. Firmy se především zaměřovaly na překlad již existujících zahraničních nemocničních informačních systémů a to především z Německé Spolkové Republiky. Jak se v běžném provozu postupem času ukázalo, pro podmínky českého zdravotnictví byly tyto systémy téměř nepoužitelné. Důvody byly jak legislativní, např. rozdílné vedení účetnictví, rozdílné vykazování poskytované péče zdravotním pojišťovnám, tak zcela praktické, spočívající ve zcela odlišné organizaci práce v nemocnicích.

### 1.1 Legislativa týkající se nemocničních informačních systémů

Hlavním legislativním podkladem pro provozování nemocničních informačních systémů je Zákon o zdravotních službách a podmínkách jejich poskytování č. 372/2011 Sb. ze dne 6. listopadu 2011 ve znění pozdějších předpisů, který stanovuje v § 53 - § 55 následující podmínky pro práci se zdravotnickou dokumentací:

#### § 53

*(1) Poskytovatel je povinen vést a uchovávat zdravotnickou dokumentaci a nakládat s ní podle tohoto zákona a jiných právních předpisů. Zdravotnická dokumentace je souborem informací podle odstavce 2 vztahujících se k pacientovi, o němž je vedena.*

*(2) Zdravotnická dokumentace podle účelu jejího zaměření obsahuje*

*a) identifikační údaje pacienta, kterými jsou jméno, popřípadě jména, příjmení, datum narození, rodné číslo, je-li přiděleno, číslo pojištění veřejného zdravotního pojištění, není-li tímto číslem rodné číslo pacienta, adresu místa trvalého pobytu na území České republiky, jde-li o cizince místo hlášeného pobytu na území České republiky a v případě osoby bez trvalého pobytu na území České republiky adresu bydliště mimo území České republiky,*

*b) pohlaví pacienta,*

- c) *identifikační údaje poskytovatele, kterými jsou jméno, popřípadě jména, příjmení poskytovatele a adresu místa poskytování zdravotních služeb v případě fyzické osoby, obchodní firmu nebo název poskytovatele, adresu sídla nebo adresu místa podnikání v případě právnické osoby, identifikační číslo, bylo-li přiděleno, název oddělení nebo obdobné části, je-li zdravotnické zařízení takto členěno,*
- d) *informace o zdravotním stavu pacienta, o průběhu a výsledku poskytovaných zdravotních služeb a o dalších významných okolnostech souvisejících se zdravotním stavem pacienta a s postupem při poskytování zdravotních služeb,*
- e) *údaje zjištěné z rodinné, osobní a pracovní anamnézy pacienta, a je-li to důvodné, též údaje ze sociální anamnézy,*
- f) *údaje vztahující se k úmrtí pacienta,*
- g) *další údaje podle tohoto zákona nebo jiných právních předpisů upravujících zdravotní služby nebo poskytování zdravotní péče.*

#### § 54

(1) *Zdravotnická dokumentace může být za podmínek stanovených tímto zákonem vedena v listinné nebo elektronické podobě nebo v kombinaci obou těchto podob. V elektronické podobě je zdravotnická dokumentace pořizována, zpracovávána, ukládána a zprostředkovávána v digitální formě s využitím informačních technologií.*

(2) *Zdravotnická dokumentace, včetně jejích samostatných součástí, musí být vedena průkazně, pravdivě, čitelně a musí být průběžně doplňována. Zápisy se provádějí bez zbytečného odkladu. Jde-li o poskytování akutní lůžkové péče, zápis o aktuálním zdravotním stavu pacienta se provádí nejméně jednou denně.*

(3) *Každý zápis do zdravotnické dokumentace vedené*

a) *v listinné podobě musí být opatřen*

1. *uvedením data jeho provedení,*

2. *podpisem zdravotnického pracovníka nebo jiného odborného pracovníka, který zápis provedl, a otiskem razítka s jmenovkou nebo čitelným přepisem jeho jména, popřípadě jmen, příjmení; to neplatí v případě poskytovatele, který poskytuje zdravotní služby vlastním jménem,*

b) v elektronické podobě musí být opatřen identifikátorem záznamu; samotný zápis obsahuje nezměnitelné, nezpochybnitelné a ověřitelné údaje, kterými jsou

1. datum provedení zápisu,

2. identifikační údaje zdravotnického pracovníka nebo jiného odborného pracovníka, který záznam provedl.

(4) Opravy zápisů ve zdravotnické dokumentaci se provádí novým zápisem. Zápis se opatří uvedením data opravy a dalšími náležitostmi podle odstavce 3. Původní zápis musí zůstat čitelný. V doplnění nebo opravě zápisu ve zdravotnické dokumentaci na žádost pacienta se uvede datum a čas provedení zápisu a poznámka, že jde o opravu nebo doplnění na žádost pacienta; zápis se opatří podpisem pacienta a zdravotnického pracovníka, který jej provedl.

#### § 55

Zdravotnickou dokumentaci lze vést pouze v elektronické podobě za splnění těchto podmínek:

a) technické prostředky použité k uložení záznamů v elektronické podobě zaručují, že údaje v provedených záznamech nelze dodatečně modifikovat; technickými prostředky jsou organizačně-technická opatření, informační systémy, technické zařízení a vybrané pracovní postupy,

b) informační systém, ve kterém je vedena zdravotnická dokumentace v elektronické podobě, eviduje seznam identifikátorů záznamů v elektronické dokumentaci pacientů vedené poskytovatelem a umožňuje jeho poskytování dálkovým přístupem,

c) bezpečnostní kopie datových souborů jsou prováděny nejméně jednou za pracovní den,

d) před uplynutím doby životnosti zápisu na technickém nosiči dat je zajištěn přenos na jiný technický nosič dat,

e) uložení kopií pro dlouhodobé uchování musí být provedeno způsobem znemožňujícím provádět do těchto kopií dodatečné zásahy; tyto kopie jsou vytvářeny nejméně jednou za kalendářní rok,

f) při uchovávání kopií pro dlouhodobé uchování na technickém nosiči dat je zajištěn přístup k těmto údajům pouze oprávněným osobám a je zajištěna jejich čitelnost nejméně po dobu, která je stanovena pro uchování zdravotnické dokumentace,

g) dokumenty v listinné podobě, které jsou součástí zdravotnické dokumentace a které vyžadují podpis osoby, jež není zdravotnickým pracovníkem nebo jiným odborným pracovníkem, musí být převedeny do elektronické podoby, která se podepíše uznávaným elektronickým podpisem osoby, která převod provedla; dokument v listinné podobě se uchová,

h) výstupy ze zdravotnické dokumentace lze převést do listinné podoby autorizovanou konverzí dokumentů,

i) informační systém, ve kterém je vedena zdravotnická dokumentace, musí umožňovat vytvoření speciální kopie uložené zdravotnické dokumentace ve formátu čitelném a zpracovatelném i v jiném informačním systému [5].

Co se týká legislativních povinností organizací, které zpracovávají osobní údaje, tak se zdravotnická zařízení musí řídit zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, který jasně stanovuje bezpečnostní požadavky na provozování informačních systémů a zabezpečení uchovávaných a zpracovávaných dat. Zdravotnická zařízení zpracovávají dle tohoto zákona citlivé údaje.

## § 9

### Citlivé údaje

*Citlivé údaje je možné zpracovávat, jen jestliže*

b) *je to nezbytné v zájmu zachování života nebo zdraví subjektu údajů nebo jiné osoby nebo odvrácení bezprostředního závažného nebezpečí hrozícího jejich majetku, pokud není možno jeho souhlas získat zejména z důvodů fyzické, duševní či právní nezpůsobilosti, v případě, že je nezvěstný nebo z jiných podobných důvodů. Správce musí ukončit zpracování údajů, jakmile pominou uvedené důvody, a údaje musí zlikvidovat, ledaže by subjekt údajů dal k dalšímu zpracování souhlas,*

c) *se jedná o zpracování při poskytování zdravotních služeb, ochrany veřejného zdraví, zdravotního pojištění a výkon státní správy v oblasti zdravotnictví podle zvláštního zákona nebo se jedná o posuzování zdravotního stavu v jiných případech stanovených zvláštním zákonem,*

d) je zpracování nezbytné pro dodržení povinností a práv správce odpovědného za zpracování v oblasti pracovního práva a zaměstnanosti, stanovené zvláštním zákonem [6].

Z výkladu zákona vyplývá, že všechna zdravotnická zařízení se při vzniku nemocničních informačních systémů řídí Zákonem o zdravotních službách a podmínkách jejich poskytování č. 372/2011 Sb. ze dne 6. listopadu 2011 ve znění pozdějších předpisů, kde vedení zdravotní dokumentace je nařízeno tímto zákonem. Nicméně zákon stanovuje obecně platné povinnosti pro zabezpečení uložených dat.

Povinnosti osob při zabezpečení osobních údajů

### § 13

(1) *Správce a zpracovatel jsou povinni přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů. Tato povinnost platí i po ukončení zpracování osobních údajů.*

(2) *Správce nebo zpracovatel je povinen zpracovat a dokumentovat přijatá a provedená technicko-organizační opatření k zajištění ochrany osobních údajů v souladu se zákonem a jinými právními předpisy.*

(3) *V rámci opatření podle odstavce 1 správce nebo zpracovatel posuzuje rizika týkající se*

*a) plnění pokynů pro zpracování osobních údajů osobami, které mají bezprostřední přístup k osobním údajům,*

*b) zabránění neoprávněným osobám přistupovat k osobním údajům a k prostředkům pro jejich zpracování,*

*c) zabránění neoprávněnému čtení, vytváření, kopírování, přenosu, úpravě či vymazání záznamů obsahujících osobní údaje a*

*d) opatření, která umožní určit a ověřit, komu byly osobní údaje předány.*

(4) *V oblasti automatizovaného zpracování osobních údajů je správce nebo zpracovatel v rámci opatření podle odstavce 1 povinen také*

- a) zajistit, aby systémy pro automatizovaná zpracování osobních údajů používaly pouze oprávněné osoby,
- b) zajistit, aby fyzické osoby oprávněné k používání systémů pro automatizovaná zpracování osobních údajů měly přístup pouze k osobním údajům odpovídajícím oprávnění těchto osob, a to na základě zvláštních uživatelských oprávnění zřízených výlučně pro tyto osoby,
- c) pořizovat elektronické záznamy, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány, a
- d) zabránit neoprávněnému přístupu k datovým nosičům [6].

Dále jsou zde stanovena přesná pravidla a povinnosti pro uživatele nemocničních informačních systémů, především povinnost zachovávat mlčenlivost o osobních údajích.

#### § 14

*Zaměstnanci správce nebo zpracovatele a jiné osoby, které zpracovávají osobní údaje na základě smlouvy se správcem nebo zpracovatelem, mohou zpracovávat osobní údaje pouze za podmínek a v rozsahu správcem nebo zpracovatelem stanoveném.*

#### § 15

*(1) Zaměstnanci správce nebo zpracovatele, jiné fyzické osoby, které zpracovávají osobní údaje na základě smlouvy se správcem nebo zpracovatelem, a další osoby, které v rámci plnění zákonem stanovených oprávnění a povinností přicházejí do styku s osobními údaji u správce nebo zpracovatele, jsou povinni zachovávat mlčenlivost o osobních údajích a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů. Povinnost mlčenlivosti trvá i po skončení zaměstnání nebo příslušných prací.*

*(2) Ustanovením předchozího odstavce není dotčena povinnost zachovávat mlčenlivost podle zvláštních zákonů.*

*(3) Povinnost zachovávat mlčenlivost se nevztahuje na informační povinnost podle zvláštních zákonů [6].*

Jak jsem již uváděl výše, je nemocnice zpracovatelem osobních údajů dle zvláštního zákona (č. 372/2011 Sb.) a proto se na zdravotnická zařízení nevztahuje oznamovací



povinnost dle § 18 zákona č. 101/2000 Sb., o ochraně osobních údajů a tuto skutečnost nemusí oznamovat Úřadu pro ochranu osobních údajů.

## 1.2 Vývoj nemocničních informačních systémů

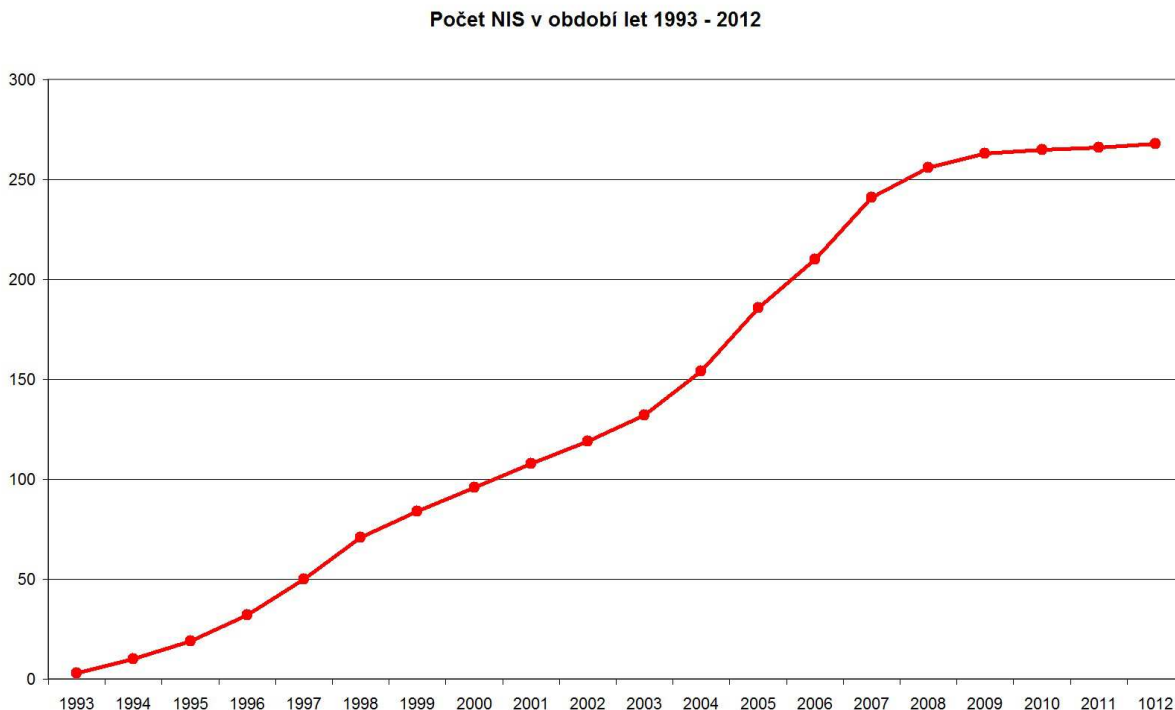
Trh s nemocničními informačními systémy se v České republice začal naplno rozvíjet v roce 1993, kdy bylo založeno velké množství firem zabývajících se vývojem vlastních ryze českých nemocničních informačních systémů. Mezi nejvýznamnější vývojáře nemocničních informačních systémů patřily následující firmy:

- AMIS, spol. s r. o. se systémem AMIS\*H
- Stapro spol. s r. o. se systémem MEDELA
- Akord Software spol. s r. o. se systémem NIS AKORD
- SMS, spol. s r. o. se systémem CLINICOM
- Medicon, a. s. se systémem GreyFox
- HiComp, a. s. se systémem NIS HiComp

U ostatních firem se jednalo převážně o lokální systémy provozované v jednotlivých nemocnicích, jejichž autory byli ve většině případů informatici příslušných zdravotnických zařízení. U všech výše uvedených vývojářů se jednalo o modulární nemocniční informační systémy, které byly ve většině případů upravovány přímo pro určité typy nemocničních zařízení. Firmy systémy vyráběly od analýzy potřeb, přes projekt, k samotné realizaci nemocničního informačního systému. Z důvodů nedostatku finančních prostředků na investice, provozovaly některé nemocnice nemocniční informační systémy formou outsourcingu.

V následující tabulce je uveden vývoj počtu provozovaných nemocničních informačních systémů ve zdravotnických zařízeních v České republice za období 1993 – 2012.

Graf 1. Vývoj počtu instalovaných systémů v ČR



Z grafu vyplývá, že v roce 2008 se trh s nemocničními informačními systémy v podstatě nasýtl a již nedochází k nasazování nových systémů.

### 1.3 Integrace firem

Vývoj na trhu s nemocničními informačními systémy se stal vzhledem ke své roztržitosti neudržitelný a na českém trhu začalo docházet ke konsolidaci a slučování softwarových firem. V současné době existují na trhu následující firmy, které zajišťují vývoj a servis nemocničních informačních systémů:

- ICZ, a. s. se systémy AMIS\*H a MPA
- Stapro, spol. s r. o. se systémy FONS, StaproMedela a StaproAkord
- CompuGroup Medical Česká republika spol. s r. o. se systémy MEDICUS, CLINICOM, CGM G3 Systema

Ostatní firmy byly postupem času integrovány do těchto tří firem a jen malé procento nemocnic zůstalo v lokálních řešení, které si vytvořili vlastními prostředky.

### 1.3.1 ICZ, a. s.

Společnost ICZ a.s. působí na trhu od roku 1998. Jejím posláním je tvorba komplexních řešení informačních technologií, systémové integrace a služeb pro zákazníky ve veřejné správě, zdravotnictví, telekomunikacích a ve stovce nejvýznamnějších společností v České republice. Mezi hlavní činnosti společnosti patří analýza, projektování a realizace informačních systémů, projekty rozsáhlých komunikačních sítí, bezpečnost informačních systémů, outsourcing informačních systémů, systémová integrace a konzultační služby. Oblast zdravotnictví je v ICZ a. s. jednou z nejvýznamnějších oblastí pro tvorbu řešení a dodávky služeb s více než 15-ti letou historií. Touto oblastí se ve firmě prioritně zabývá divize Zdravotnictví a samozřejmě ve spolupráci s ostatními divizemi, především s divizí Sítě a divizí Bezpečnost. ICZ a. s. je tedy jako jedna z mála firem na trhu schopná dodávat zákazníkům v oblasti Healthcare ucelená komplexní řešení v celé šíři IT potřeb [15].

### 1.3.2 Stapro, spol s r. o.

Společnost Stapro s. r. o. je významným dodavatelem informačních systémů a zároveň i poskytovatelem služeb v oblasti informačních technologií pro zdravotnictví. V roce 1993 se její působení přeneslo i na Slovensko, kde byla založena dceřiná společnost STAPRO Slovensko s. r. o. Společnost Stapro sídlí v Pardubicích a v rámci České republiky má pobočky v Praze, Liberci a také v Ostravě.

Jedním z hlavních cílů společnosti je rozšiřovat počty zákazníků nejen na domácích trzích, ale i v rámci střední a východní Evropy a ve spolupráci s nimi vytvářet „best practices“ organizace a informační podpory procesů ve zdravotnictví.

V současné době Stapro disponuje nejkompexnějším portfoliem produktů a služeb na trhu české a slovenské zdravotnické informatiky, které pokrývá následující oblasti:

- aplikované konzultační služby pro zvýšení kvality a efektivity zdravotnických procesů
- integrované a funkčně provázané produkty pokrývající informační potřeby zdravotnického zařízení v klíčových procesech a umožňující realizaci a měření konzultačních doporučení

- služby zavedení informačního systému a podpory provozu
- služby zajištění dostupnosti a bezpečnosti informační infrastruktury, SLA služby a služby kompletního převzetí péče o informační systémy (outsourcing)

Zákazníci a partneři Stapro vnímají jako silnou, profesionální a dobře prosperující firmu. Veškeré produkty a služby poskytované společností Stapro s. r. o. jsou založeny na certifikovaných procesech podle systému řízení jakosti ISO 9001:2000. Stapro je také držitelem certifikátu environmentálního systému řízení dle ISO 14001:2004 a klade tak velký důraz na to, aby všechny aktivity byly co nejvíce ohleduplné k životnímu prostředí. Od září 2007, kdy byl zaveden systém bezpečnosti informací, je Stapro s. r. o. schopno aktivně vyhodnocovat svá rizika na poli ochrany informací a efektivně uplatňovat kontrolní a řídicí mechanismy k zachování důvěrnosti, integrity a dostupnosti těchto informací. Podařilo se nastavit ochranné mechanismy tak, aby rizika spojená s únikem firemních informačních aktiv a aktiv firemních zákazníků byla minimalizována.

V souladu se strategií rozšiřování svých služeb (v roce 2005 se uskutečnilo spojení se společností Akord) se na začátku roku 2008 společnost Stapro s. r. o. stala 100 % vlastníkem společnosti MLAB software s. r. o. Cílem tohoto kroku je integrovat aktivity pro laboratorní komplement do jedné společnosti. Fúze umožní koncentrovat a synergicky využít odborné kapacity obou týmů v oblasti informační podpory zdravotnického laboratorního komplementu. Zároveň se také zefektivní rozvoj nové generace informačního systému OpenLIMS a bude zajištěn kvalitativní rozvoj v oblasti mikrobiologie [16].

### **1.3.3 CompuGroup Medical Česká republika, spol. s r. o.**

CompuGroup Medical je mezinárodní softwarová společnost zaměřená na oblast zdravotnictví. Všechny firemní produkty a systémy jsou zaměřeny jedním směrem a to umožnit komukoliv přístup k jeho zdravotním záznamům, kdykoliv a kdekoliv, za účelem toho nejlepšího možného léčebného postupu. Společnost CompuGroup Medical Česká republika s. r. o., jako dodavatel komplexních řešení IT pro zdravotnictví, nabízí portfolio produktů a služeb, pokrývajících široké spektrum činností a potřeb zdravotnických zařízení všech typů a velikostí. Jednotlivé produkty dodávané holdingem CompuGroup Medical je

možno samozřejmě integrovat do ucelených řešení, ať již je to prostřednictvím původní proprietární komunikace, komunikace na bázi všeobecně uznávaných národních a mezinárodních datových standardů, nebo o integraci s různorodými informačními systémy třetích stran realizovanou prostřednictvím integračních nástrojů. CompuGroup Medical Česká republika samozřejmě poskytuje svým zákazníkům maximální podporu provozu a údržbu všech používaných informačních systémů. Pro příjem požadavků je k dispozici Help Desk s odpovídající metodikou pro příjem a řízení zpracování požadavků zákazníků [17].

#### 1.4 Národní zdravotní systém

Již od počátku elektronizace zdravotnictví byly snahy o zavedení centrálního celorepublikového informačního systému, který by uchovával veškeré zdravotnické informace. V roce 2001 založila Všeobecná zdravotní pojišťovna společnost IZIP, a. s., která měla tyto představy celorepublikového zdravotnického informačního systému realizovat. Elektronická zdravotní knížka se stala vysoce zabezpečeným souhrnem zdravotních informací pacienta v elektronické podobě, která byla přístupná 24hodin denně prostřednictvím internetu. Zároveň se jednalo o bezpečné prostředí propojující poskytovatele zdravotní péče, pacienty a zdravotní pojišťovny. Sloužilo k předávání zdravotních informací mezi lékařem a pacientem a mezi lékaři navzájem, v nouzových případech může pomoci zachránit život. Její vedení i zřízení je v současné době zdarma pouze pro pojištěnce VZP ČR. Princip elektronické zdravotní knížky tak spočíval ve smysluplném sdílení nejaktuálnějších informací o zdravotním stavu pacientů zdravotnickými pracovníky, kterým to pacient umožnil. Podobně jako fungovala léčba v praxi. Výhodou elektronické zdravotní knížky, která byla nespornou výhodou pro pacienty bylo to, že lékař bude mít vždy v pravý čas k dispozici pacientovu kompletní zdravotní historii, kterou se souhlasem pacienta mohl doplňovat o aktuální zdravotní záznamy. Lékaři tímto byla usnadněna práce a čas, který pro správné rozhodnutí potřeboval [18]. Bohužel z politických a zcela praktických důvodů se představy Ministerstva zdravotnictví ČR a společnosti IZIP a. s., nenaplnily a z rozhodnutí vlády se projekt internetových zdravotních knížek v roce 2012 v podstatě zastavil a další vývoj byl ukončen. Jedním z hlavních důvodů bylo nedostatečné technické vybavení ordinací lékařů,

dále v době svého vzniku malý počet obyvatelstva s přístupem k internetu a posledním důvodem bylo zpoplatnění přístupu pro pacienty jiných zdravotních pojišťoven (zdarma zůstal pouze pro pojištěnce Všeobecné zdravotní pojišťovny). Ministerstvo zdravotnictví ČR v současné době připravuje podklady pro veřejnou zakázku na software, který by měl projekt IZIP nahradit.

## 2 OBECNÝ POPIS NEMOCNIČNÍHO INFORMAČNÍHO SYSTÉMU

Nemocniční informační systémy v současné době pokrývají veškeré zdravotnické i nezdravotnické provozy nemocnice (klinická část, lůžková oddělení, urgentní příjem, ambulance, operační sály, hematologickou laboratoř, biochemickou laboratoř, mikrobiologickou laboratoř, patologickou laboratoř, transfuzní službu, radiodiagnostické oddělení, lékárnu, pojišťovnu, statistiku ÚZIS, účetnictví, fakturaci, personalistiku, mzdovou agendu, skladovou agendu, stravovací provoz a prádelnu). Primárním úkolem komplexních informačních systémů je centralizace veškerých dat zpracovávaných v nemocničním informačním systému. Integrojícím prvkem je kompatibilita dat, která umožňuje komunikaci mezi moduly uvnitř nemocničního informačního systému i vazbu na vnější struktury prostřednictvím datových standardů [3]. Ve většině případů se jedná o komplexní řešení dodávané jedním softwarovým integrátorem.

### 2.1 Klinické moduly

Klinické moduly zpracovávají odborná data, která se týkají diagnostických a léčebných procesů. Jedná se o základní agendu vedení zdravotnické dokumentace v nemocničním informačním systému, ve které jsou sdružována veškerá data pacientů.

#### 2.1.1 Lůžkové oddělení

V tomto modulu jsou vytvářeny základní dokumenty zdravotnické dokumentace, jedná se především o základní identifikační údaje pacienta, vstupní anamnézu, stav při přijetí, průběh hospitalizace, epikrízu, souhrn veškerých diagnóz, laboratorní vyšetření v průběhu hospitalizace, ambulantní zprávy konzilií, obrazová data z radiodiagnostického oddělení, přehled ordinovaných léků a infuzí, operační zprávy, závěrečné propouštěcí zprávy. Důležitou součástí tohoto modulu je část zabývající se vyúčtováním poskytnuté zdravotní péče zdravotním pojišťovnám. Mezi základní funkcionalitu modulu patří automatické generování závěrečné propouštěcí zprávy, do které lékař dopisuje pouze závěr a doporučení další léčby. Nedílnou součástí modulu lůžkového oddělení je část věnovaná sesterské (ošetřovatelské) péči, která byla v minulosti v oblasti nemocničních informačních systémů podceňována. U moderních informačních systémů jsou v současné době předávána do nemocničního informačního systému také data ze speciálních prostředků zdravotnické

techniky. Jedná se o výstupní data z monitorovacího systému (EKG, EEG, SpO2, atd.), plicních ventilátorů, injekčních a infuzních dávkovačů.

```

ODD:  Hos Prop Zal.ch novÍ poJ paC voL_s Vý pRo Ná
=(ARO)==== (batka)===== (6) ==
HOSPITALIZOVANÍ PACIENTI
-----
Po. Lu. Příjmení, jméno      Roč. Příjem   Dg      Dieta      žád/výsl
-----
1  1  OTÝPKA JIŘÍ                23.04.13    R402
1  2  KONČELÍK KAREL            01.04.13    J969
2  1  NAVRÁTIL PETR              25.04.13    J180
2  2  KADLEC VÁCLAV              27.04.13    G122
3  1  GYBASOVÁ EDITA            23.04.13    K319
3  2  GERGEL MILAN               19.04.13    I638
-----
-----Celkem      6 pacientů
Výběr z hospitalizovaných pacientů

```

Obr. 1. Modul lůžkového oddělení

### 2.1.2 Ambulance

Modul shromažďuje veškeré informace o ambulantním vyšetření a to včetně veškerých navazujících laboratorních vyšetření a radiodiagnostických obrazových dat. Součástí ambulantních modulů je část určená pro plánování návštěv pacientů, která slouží k sestavení časového plánu a tím k optimalizaci provozu ambulance. Důležitá je vazba na modul lůžkového oddělení, kde při konziliárním vyšetření dochází k automatickému přenosu výsledků vyšetření. Stejně jako u modulu lůžkového oddělení je nedílnou součástí část zabývající se vyúčtováním poskytnuté zdravotní péče pojišťovnám. Zde je ale možné, na rozdíl od lůžkového oddělení, implementovat část automatického vyúčtování, neboť se jedná o poměrně jednodušší agendu, než při složitém vyúčtování hospitalizační péče.





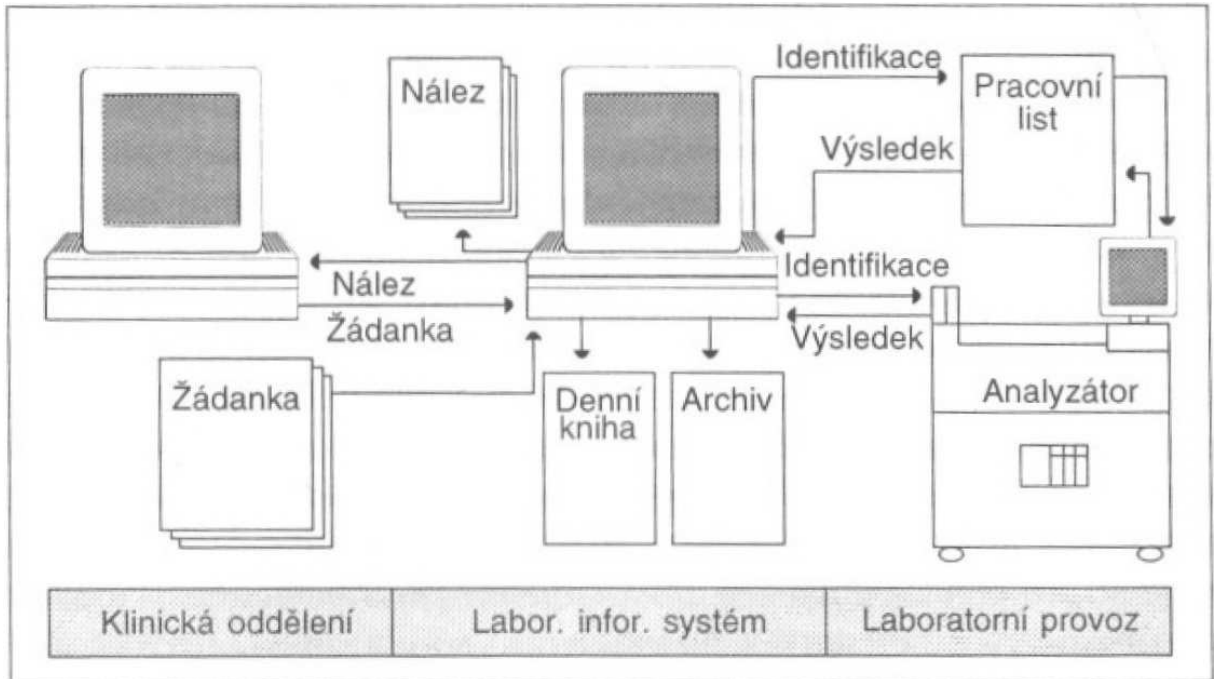
Obr. 2. Modul ambulance

### 2.1.3 Laboratoře

Co se týká produkce objemu dat, patří tento modul obecně k největším producentům. Laboratoře můžou generovat až 40 % dat nemocničního informačního systému. Tento modul je obousměrně napojen jak na klinické moduly lůžkového oddělení a ambulance, tak na laboratorní analyzátoři, které zpracovávají výsledky vyšetření.



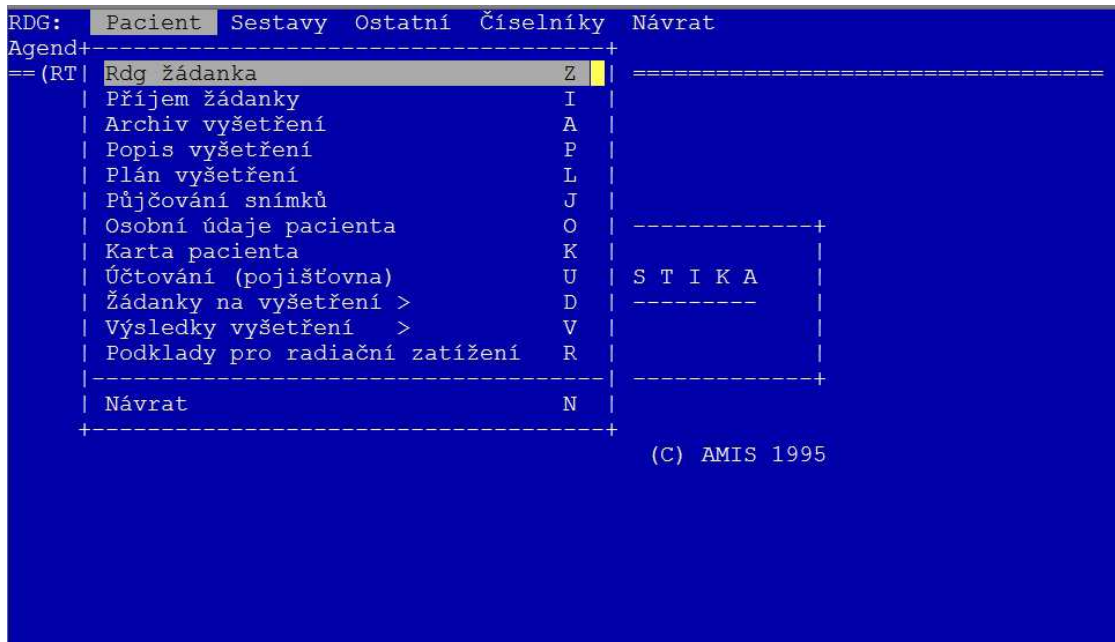
Obr. 3. Modul biochemické laboratoře



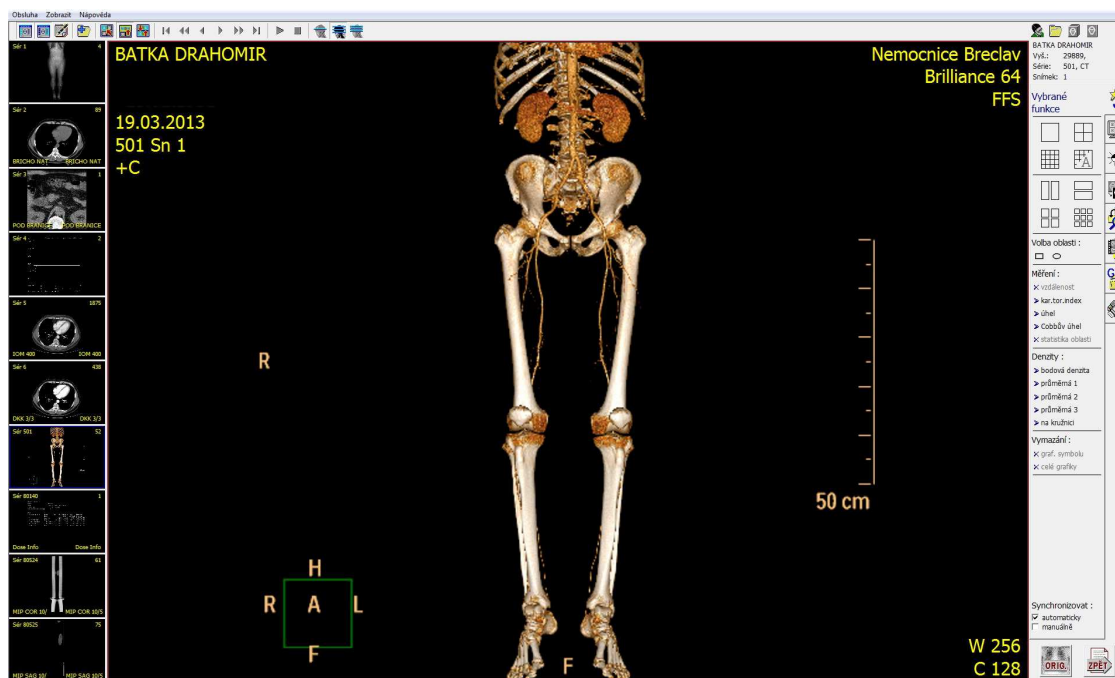
Obr. 4. Blokové schéma toku dat [3]

#### 2.1.4 Radiodiagnostické oddělení

Modul radiodiagnostického oddělení zažil v poslední době největší rozvoj. Důvodem bylo schválení datového standardu DICOM, na základě kterého je možné přenášet, zpracovávat a archivovat obrazová data pacientů různými modalitami. Data pacientů jsou vytvářena různými vyšetřovacími modalitami např. magnetickou rezonancí, CT přístrojem, skiagraficko-skiaskopickým přístrojem, angiografickým přístrojem a ultrazvukem. Tyto data jsou následně ukládána do speciálního modulu nemocničního informačního systému, který se obecně nazývá PACS (Picture Archiving and Communicating System).



Obr. 5. Modul radiodiagnostického oddělení



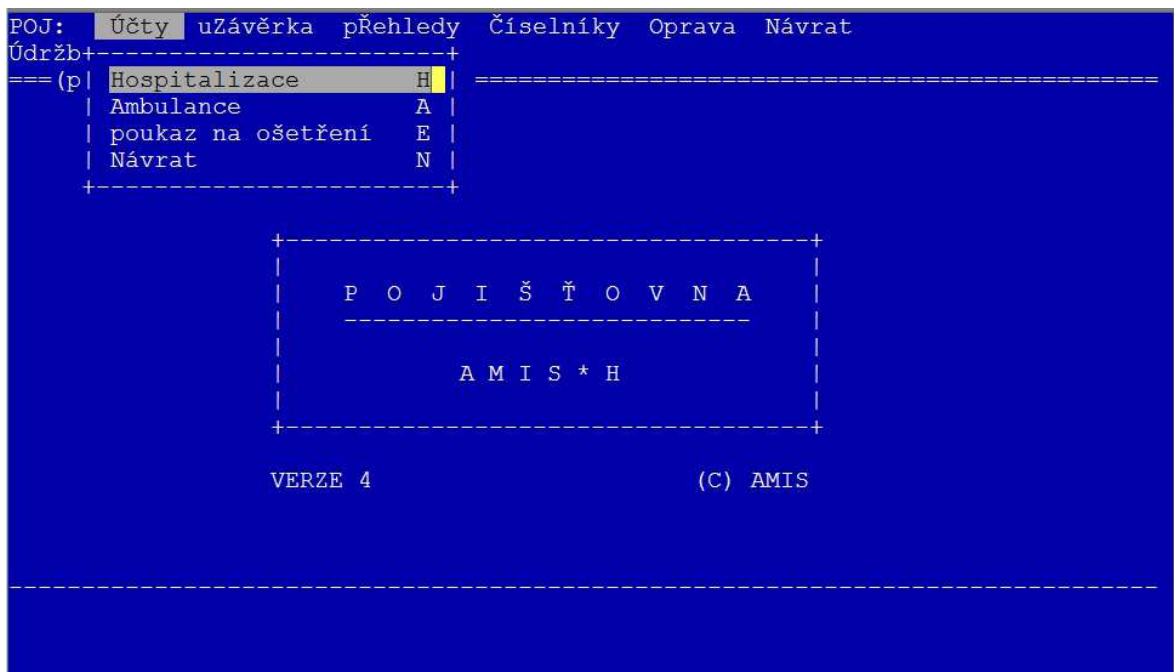
Obr. 6. Ukázka obrazových dat

## 2.2 Administrativní moduly

V této části nemocničního informačního systému se zpracovávají ostatní údaje, které jsou nezbytné pro bezproblémové fungování zdravotnického zařízení. Jedná se především o ekonomické moduly a modul, ve kterém se zpracovávají data poskytnuté zdravotní péče.

### 2.2.1 Pojišťovna

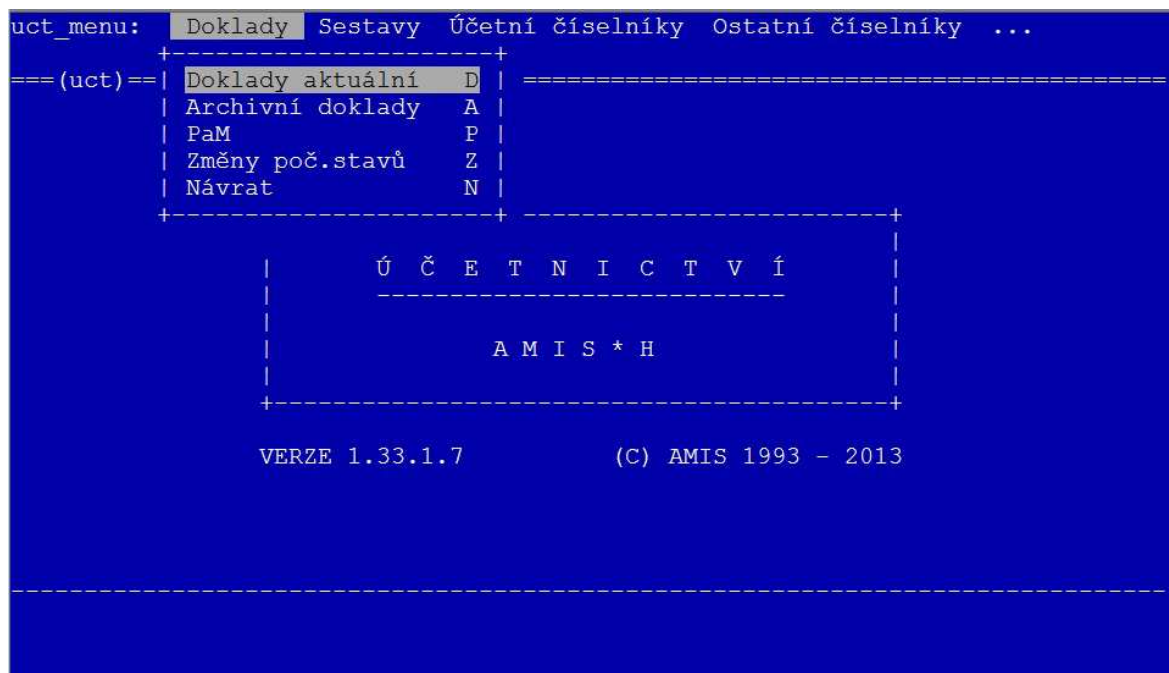
V tomto modulu dochází k shromažďování a zpracovávání veškerých dat nutných pro vykázání poskytnuté zdravotnické péče, poskytnutých léků a použití speciálního zdravotnického materiálu. Data za vykázanou lůžkovou a ambulantní péči jsou většinou pořizována administrativní pracovníci na každém oddělení, kdežto laboratorní a radiodiagnostická data jsou účtována automaticky. Automatické účtování se provádí na základě vazby mezi prováděným vyšetřením a kódem výkonu zdravotní pojišťovny. Veškerá data jsou zdravotním pojišťovnám předávána prostřednictvím zabezpečených internetových portálů ve formě tzv. K-dávek (jedná se o přesně nadefinovaný textový soubor, který se vytváří pro každou zdravotní pojišťovnu samostatně).



Obr. 7. Modul zdravotní pojišťovny pojišťovny

### 2.2.2 Účetnictví

Tento modul zpracovává ekonomická data pro celé zdravotnické zařízení dle platné legislativy. Součástí modulu jsou podsystemy fakturace, pokladny, komunikace s bankou, operativní evidence, skladové hospodářství. Tento modul je napojen na modul mzdové agendy a mzdová data jsou automaticky přenášena do modulu účetnictví. Výstupem jsou sestavy hlavní účetní knihy, výsledovky, výkaz zisku a ztrát atd.



Obr. 8. Modul účetnictví

## 2.3 Provozní moduly

Jedná se o podpůrné moduly nemocničního informačního systému s vazbami na klinické moduly a z části i na administrativní moduly.

### 2.3.1 Stravovací provoz

Modul umožňuje dietním sestřám efektivně sestavit plán jídelniček a rozvrhy stravy pro jednotlivé pacienty. Diety ordinované na oddělení slouží jako požadavky pro výdej ze skladu potravin na základě předepsaných norem stravy. Pohyb materiálu mezi dodavateli a skladem na jedné straně a skladem a kuchyní na druhé straně je standardní úloha skladového hospodářství a toto řešení pomocí nemocničního informačního systému přináší do hospodaření transparentní relace a zlepšuje plynulost zásobování [3].

```

NABÍDKA: Požadavky Číselníky nástroje Návrat
Zadávání požadavků kuchyni
==(kch)=+-----+=====
|                                     |
|          Požadavky                 |
|-----+-----+-----+
| Diety - požadavky na diety         D |
| Stravenky - zadávání požadavků     S | -----+
|-----+-----+-----+
| Sumování změn požadavků           Z | V O Z |
| Výpis požadavků za celou nemocnici C | -----|
| Výpis požadavků po odděleních      O |
| Výpis součtu všech požadavků      Q |
| Výpis požadavků na výdej.pás       V |
| Výpis po odděleních + stravenky    W | -----+
| Výpis po odděleních bez stravenek  B |
| Výpis požadavků na stravenky       T | 993 - 1998
| Výpis všech jímenovitě            J |
| Výpis všech přídávků              K |
| Nové požadavky od půlnoci do rána R |
| Náklady na stravu dle stanov.cen   L |
|-----+-----+-----+
| Návrat                             N | -----+
+-----+-----+

```

Obr. 9. Modul stravovacího provozu

### 2.3.2 Dopravní zdravotní služba

Modul prostřednictvím žádanek a převozních lístků zajišťuje komunikaci mezi klinickými moduly lůžkové a ambulantní složky nemocničního informačního systému a moduly dispečinku dopravní zdravotní služby, případně ze střediskem rychlé zdravotnické pomoci.

```

DOPRAVA: Dispečink Číselníky Konfigurace Návrat
==(dpd)==-----+=====
|          DISPEČINK                 |
|-----+-----+-----+
| DZS                                D |
|-----+-----+-----+
| Návrat                             N |
+-----+-----+-----+
|                                     |
|          D O P R A V A           |
|          -----                 |
|          A M I S * H             |
|                                     |
+-----+-----+-----+
|                                     |
|          VERZE 1.0                |
|                                     |
|          (C) AMIS 1995            |
|                                     |
+-----+-----+-----+

```

Obr. 10. Modul dopravní zdravotní služby

## 2.4 Správa systému

Jedná se o samostatný modul, který má za úkol přidělování vstupu a přístupových práv k jednotlivým modulům nemocničního informačního systému. V tomto modulu jsou vytvářeny vazby mezi jednotlivými moduly. V modulu mohou být definovány přístupy jednotlivých uživatelů až na úroveň chorobopisu případně ambulantního záznamu. Modul zajišťuje filtrování přístupových informací mezi subsystémy nemocničního informačního systému.

```
POV:  Chor_č  Amb_č  cHor  aMb  Priv_u  naSt  Návrat
-----
+-----+
| P Ř Í S T U P O V Á   P R Á V A   K   D O K U M E N T A C I |
|-----|
|                   A M I S * H                               |
+-----+
VERZE 1.0                                                    (C) AMIS 1997
-----
Časově omezené povolení přístupu do chorobopisů.
```

Obr. 11. Modul správy systému

### 3 ZÁKLADNÍ DEFINICE TÝKAJÍCÍ SE BEZPEČNOSTI NEMOCNIČNÍCH INFORMAČNÍCH SYSTÉMŮ

1. **Dostupnost** – zajištění, že informace je pro oprávněné uživatele přístupná v okamžiku její potřeby
2. **Důvěrnost** – zajištění, že informace jsou přístupné nebo sděleny pouze těm, kteří jsou k tomu oprávněni
3. **Bezpečnost informací** – zachování důvěrnosti, integrity a dostupnosti informací a dalších vlastností, jako např. autentičnost, odpovědnost, nepopíratelnost a spolehlivost
4. **Integrita** – zajištění správnosti a úplnosti informací
5. **Osobní údaj** - 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
6. **Citlivý údaj** - osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj subjektu údajů
7. **Anonymní údaj** - takový údaj, který buď v původním tvaru nebo po provedeném zpracování nelze vztáhnout k určenému nebo určitelnému subjektu údajů
8. **Subjekt údajů** - fyzická osoba, k níž se osobní údaje vztahují – pacient
9. **Zpracování osobních údajů** - jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky. Zpracováním osobních údajů se rozumí zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace



10. **Shromažďování osobních údajů** - systematický postup nebo soubor postupů, jehož cílem je získání osobních údajů za účelem jejich dalšího uložení na nosič informací pro jejich okamžité nebo pozdější zpracování
11. **Uchovávání osobních údajů** - udržování údajů v takové podobě, která je umožňuje dále zpracovávat
12. **Blokování osobních údajů** - vytvoření takového stavu, při kterém je osobní údaj určitou dobu nepřístupný a nelze jej jinak zpracovávat
13. **Likvidace osobních údajů** - fyzické zničení jejich nosiče, jejich fyzické vymazání nebo jejich trvalé vyloučení z dalších zpracování
14. Organizace svými vnitřními předpisy, v souladu s platnou legislativou, určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj. Zpracováním osobních údajů jsou pověřeni zaměstnanci organizace dle stanovených náplní práce, odpovědností a kompetencí.
15. **Evidence nebo datový soubor osobních údajů** - jakýkoliv soubor osobních údajů uspořádaný nebo zpřístupnitelný podle společných nebo zvláštních kritérií.
16. Kategorie rozsahu přístupu k osobním a citlivým údajům pacientů pro jednotlivé zaměstnance, skupiny zaměstnanců a třetí osoby v rozsahu:
  - a. Kategorie A – přístup v plném rozsahu
  - b. Kategorie B – přístup v rozsahu dle legislativy, souhlasu pacienta
  - c. Kategorie C – přístup v nezbytném rozsahu pro zajištění výkonu činností dle stanovené odpovědnosti
  - d. Kategorie D – přístup pouze k vybraným údajům; v rozsahu nezbytném pro zajištění výkonu činností, např. dle stanovených kritérií auditu, kontroly, provedení analýzy.

### 3.1 Bezpečnostní hrozby nemocničních informačních systémů

Bezpečnostní hrozby týkající se zabezpečení nemocničních informačních systémů provozovaných na linuxových platformách se nezaměřují na hrozby klasických informačních systémů provozovaných na systémech platformy Windows. V linuxových nemocničních informačních systémech se problematika virové hrozby řeší pouze na úrovni uživatelských pracovních stanic, protože se v tomto případě jedná o terminálový provoz a pracovní stanice funguje pouze jako terminál. Ochrana se tak obecně zaměřuje hlavně na ochranu proti tzv. „vnitřnímu nepříteli“ a optimálnímu zabezpečení vnitřního chodu nemocničního informačního systému. Jedná se o optimalizaci zabezpečení TCP/IP provozu nastavením VLAN, filtrování provozu datové sítě a nemožnost připojení neregistrovaných IP adres. VTP (VLAN Trunking Protocol) je protokol využíváný pro distribuci VLAN (konfiguračních parametrů) v přepínaných sítích. V praxi to znamená, že definice VLAN je provedena na jednom centrálním místě a následně jsou tyto informace šířeny na veškeré přepínače v lokální síti, které sdílí stejnou VTP doménu. Jako u všech informačních systémů tak i u nemocničních informačních systémů jsou nejslabším bezpečnostním místem samotní uživatelé. Nedisciplinovanost uživatelů při zadávání hesla a neodhlašování se ze systému je považováno za jednu z největších bezpečnostních „děr“ do nemocničního informačního systému.

V praktické části diplomové práce se na základě výše uvedených legislativních požadavků a dlouhodobých zkušeností z rutinního provozu nemocničního informačního systému v Nemocnici Břeclav, p.o., zaměřím na návrh a optimalizaci provozu VLAN, vypracování detailního seznamu IP adres a optimalizaci aplikační části.

## **II. PRAKTICKÁ ČÁST**

## 4 NEMOCNIČNÍ INFORMAČNÍ SYSTÉM AMIS\*H

Nemocniční informační systém AMIS\*H byl implementován již v roce 1994 a jako jediný informační systém v té době pokrýval veškeré zdravotnické i nezdravotnické provozy nemocnice (lůžková oddělení, ambulance, laboratoře, radiodiagnostické oddělení, pojišťovnu, statistiku ÚZIS, účetnictví, fakturaci, personalistiku, skladovou agendu, stravovací provoz a prádelnu). Komplexním dodavatelem hardware i software byla brněnská firma AMIS spol. s r. o. (ADVANCED MEDICAL INFORMATION SYSTEMS), která byla postupem času integrována do společnosti ICZ a.s.. Již od začátku nemocnice vsadila na tehdy již osvědčenou platformu HP UNIX – INFORMIX. Prvotní instalace systému byla i přes tehdy platné legislativní bariéry ze strany USA (na dodávané technologie platily celní a legislativní omezení týkající se dodávek do zemí bývalého „sovětského bloku“), implementována na server HP 9000 G40 osazený riscovými procesory PA-7000 (64MHz), pamětí 384 MB a čtyřmi SCSI disky o celkové kapacitě 400 MB. Zálohování bylo prováděno na DAT pásky. Jako koncová pracoviště pro uživatele byly instalovány alfanumerické terminály WYSE – 160. Při dalším rozšiřování byly používány především z ekonomických důvodů terminály DEC DORIO.



Obr. 12. Server HP 9000 G40

Potupně samozřejmě dochází k nahrazování zastaralých alfanumerických terminálů osobními počítači. Impulzem pro radikální přechod od alfanumerických terminálů byla kompletní digitalizace radiodiagnostického oddělení. Pro digitalizaci radiodiagnostického provozu si nemocnice vybrala firmu OR-CZ s. r. o. se systémem MARIE PACS. Do systému byly v první fázi napojeny pouze dvě radiodiagnostické modalitě a to CT

Siemens a angiografický přístroj GE. Za tento projekt Nemocnice Břeclav získala významné ocenění IT projekt roku 2004 udělované Českou asociací manažerů informačních technologií ([http://www.cacio.cz/vyhlaseni\\_souteze\\_2004/](http://www.cacio.cz/vyhlaseni_souteze_2004/)). Upgradem přístrojového vybavení, které proběhlo v roce 2009 na základě přidělené dotace z evropských fondů ROP Jihovýchod, byly do PACSového systému zapojeny veškeré modality radiodiagnostického oddělení: CT Philips, skiografický přístroj Philips, skiografický přístroj GE, ultrazvukový přístroj GE a angiografický přístroj GE. V další fázi rozšiřování tohoto systému počítá nemocnice s napojením na modality ostatních zdravotnických oddělení, na kterých jsou používány především ultrazvukové přístroje.



Obr. 13. Úvodní stránka nemocničního informačního systému AMIS\*H

Páteřní infrastruktura byla vybudována tlustým koaxiálním ethernetovým spojením o rychlosti 10 MBps HD. Pomocí trancieverů byly do páteřní sítě připojeny osmi nebo šestnácti portové rozbočovače 3COM. Jako terminálové servery byly vybrány stabilní produkty Emulex Performance 4000 v 16-ti nebo 32 portovém provedení. Jakékoliv zabezpečení VLAN nebylo v té době možné a navíc s rozvojem internetu bylo připojení nemocničních informačních systémů do internetu zakázáno vyhláškou ministerstva zdravotnictví. Jediným zabezpečovacím prvkem v té době bylo přidělení loginů jednotlivým uživatelům v systému HP-UX (verze 9.04) a částečné omezení přístupů na úrovni aplikací.

Postupem času docházelo k hardwarovým obměnám serverů, ale striktně se nemocnice držela osvědčené platformy HP s riscovým procesory a to až po řadu HP RP 5470 (4x procesor PA-8700 750MHz, 16 GB RAM, 4x 16GB Ultra2 SCSI HDD). Zálohování se provádělo na DTL páskovou mechaniku.

#### 4.1 Upgrade centrálního serveru

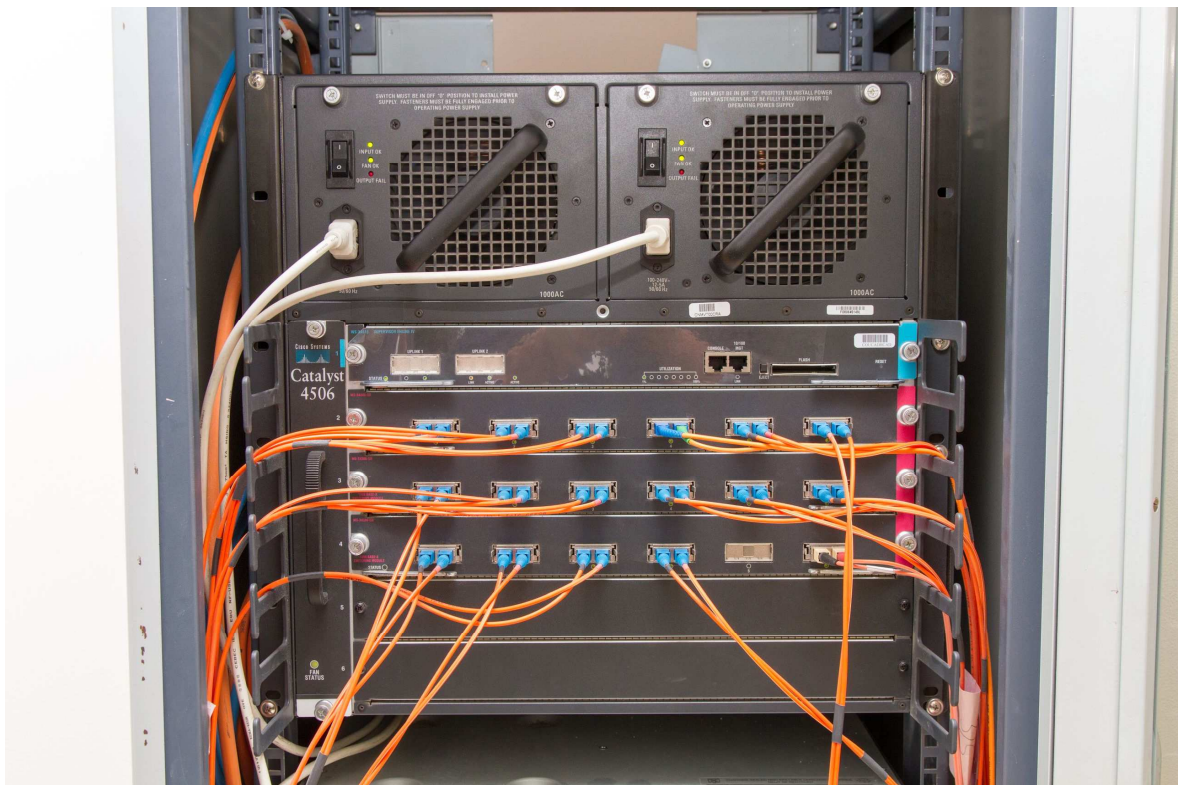
V roce 2011 byl ve spolupráci se společností ICZ a. s. proveden upgrade serveru a databázového prostředí. Bohužel především z ekonomického hlediska musela nemocnice opustit 17 let používanou riscovou architekturu centrálního serveru. Stávající konfigurace serveru je HP Integrity rx2800 i2 4-jádrový procesor Intel Itanium 9320 1,46 GHz, 32 GB RAM DDR3, pevné disky 4 x 146 GB 15k RPM (2,5") Hot-plug, HP rx2800 i2 Redundant Power Supply. Jako zálohovací mechanika byla dodána externí DAT 160. Byl nainstalován operační systém HP-UX 11i v3. Podstatná změna byla provedena i v databázovém prostředí, kde byl nainstalován IBM Informix Dynamic Server verze 11.70.FC3. Jako aplikační prostředí byl nainstalován Informix Run Time 4GL překladač verze 7.20.UD6. Pro správu databáze je nyní používán Informix ISQL development verze 7.50.FC5.



Obr. 14. HP Integrity server rx2800 i2

## 4.2 Upgrade datové sítě

V roce 2004 byla komplexně zrekonstruována datová síť. Nemocnice přešla ze zastaralé ethernetové struktury do optické struktury páteřních rozvodů. Centrální prvek CISCO CATALYST 4506 umožnil hvězdicové propojení jednotlivých pavilonů nemocnice rychlostí 1Gbps. Zastaralé rozbočovače 3COM byly kompletně nahrazeny přepínači CISCO CATALYST 2950 a to v 24 nebo 48 portové konfiguraci. Vzhledem k ještě hojně používaným alfanumerickým terminálům (WYSE-16, DEC DORIO) byly v síti zachovány terminálové servery Emulex Performance 4000. Nemocnice je do internetu připojena prostřednictvím hardwarového firewallu rychlostí 100 Mbps.



Obr. 15. Přepínač CISCO CATALYST 4506

## 5 SWOT ANALÝZA

<b>Silné stránky</b>	<b>Slabé stránky</b>
Páteřní optické rozvody	Nedostatečné zabezpečení VLAN
Jednoduchá administrativa	Nedisciplinovanost uživatelů
Unifikované uživatelské rozhraní	Není vypracován seznam IP adres
Terminálový provoz	Nízká datová propustnost koncových pracovišť
<b>Hrozby</b>	<b>Příležitosti</b>
Napadení systému hackery	Elektronická komunikace s ostatními nemocnicemi
Nebezpečí ze strany "vnitřního nepřítele"	Export dat do národních registrů
Výpadek serveru	Zvýšení konkurenceschopnosti v oblasti poskytování zdravotní péče

Mezi silné stránky nemocničního informačního systému patří vybudované páteřní rozvody s dostatečnou kapacitou mezi aktivními prvky sítě a dostatečně předimenzovaný počet záložních optických vláken. Další silnou stránkou je relativně jednoduchá administrativa celého systému, kdy je možno přistupovat k centrálnímu serveru a všem aktivním prvkům sítě z kteréhokoliv koncového pracoviště nemocničního informačního systému. Velkou výhodou pro uživatele je unifikované pracovní prostředí a terminálový provoz, což umožňuje možnost pracovat se všemi moduly nemocničního informačního systému z libovolného koncového pracoviště (alfanumerického terminálu nebo PC).

Slabou stránkou nemocničního informačního systému je nedostatečné zabezpečení VLAN, kdy jsou všechny používané IP adresy na stejné úrovni a není řešen přístup mezi



jednotlivými VLAN. Slabou stránkou je i nedisciplinovanost uživatelů při práci s nemocničním informačním systémem, kdy bez odhlášení (ukončení práce se systémem) odcházejí od pracovní stanice, případně pracují na jednoho přihlášeného uživatele. Dále nemá nemocnice vypracován podrobný seznam všech používaných adres, který by byl aplikovatelný do nemocničního informačního systému. Slabou stránkou je i nízká propustnost datové sítě ke koncovým pracovištím (100 Mbps), kdy se především po dokončení kompletní digitalizace radiodiagnostického oddělení projevila nedostatečná kapacita připojení při přenosu obrazových dat.

Tak jako u všech informačních systémů je největší hrozbou napadení systému hackery, proto je celý nemocniční informační systém připojen k internetu prostřednictvím hardwarového firewallu CISCO a je povolen pouze http provoz a všechny ostatní porty jsou na vstupu do nemocnice zakázány. Navíc běžní uživatelé přistupují na internet prostřednictvím proxy serveru a portu 5080. Pojem nebezpečí ze strany „vnitřního nepřítele“ je druh hrozby, kdy je reálné nebezpečí napadení systému z nemocnice připojením na koncové pracoviště případně nahrazení koncového pracoviště zařízením vneseným. Takto může teoreticky dojít k napadení databáze nemocnice a zneužití získaných dat. Možnou hrozbou je i výpadek centrálního serveru a to ať z důvodu dlouhodobého výpadku napájení nebo selhání hardware. Napájení je zajištěno předimenzovaným záložním zdrojem umožňujícím více než tři hodinový provoz s další možností napojení na centrální záložní zdroj napájení. Pro případ hardwarové selhání má Nemocnice Břeclav uzavřenu servisní smlouvu se společností ICZ, a. s., kdy je určen servisní zásah do čtyř hodin od oznámení havárie.

Jednou z příležitostí je možnost komunikace s ostatními zdravotnickými zařízeními prostřednictvím datových standardů a možnost výměny dat. V dnešní době je Nemocnice Břeclav připojena k celorepublikovým nemocničním informačním systémům výměny a sdílení radiodiagnostických obrazových dat a to k systémům ePacs a Redimed. Dále je možné informační systém připojit prostřednictvím datových standardů do národních systémů hlášení hospitalizací, rodiček a novorozenců, případně jiných externích systémů, které splňují datové standardy. Příležitostí je vzhledem ke komplexnosti nemocničního informačního systému zvýšení konkurenceschopnosti Nemocnice Břeclav v oblasti poskytování celého spektra zdravotní péče s datovou provázaností všech provozů nemocnice. Tímto dochází především k ekonomickým úsporám a eliminaci chybných

exportovaných dat, které nemocnice předává například ve formě laboratorních výsledků externím zdravotnickým zařízením.

Řešení optimalizace zabezpečení

Na základě vypracované SWOT analýzy můžeme zabezpečení nemocničního informačního systému rozdělit do tří základních oblastí:

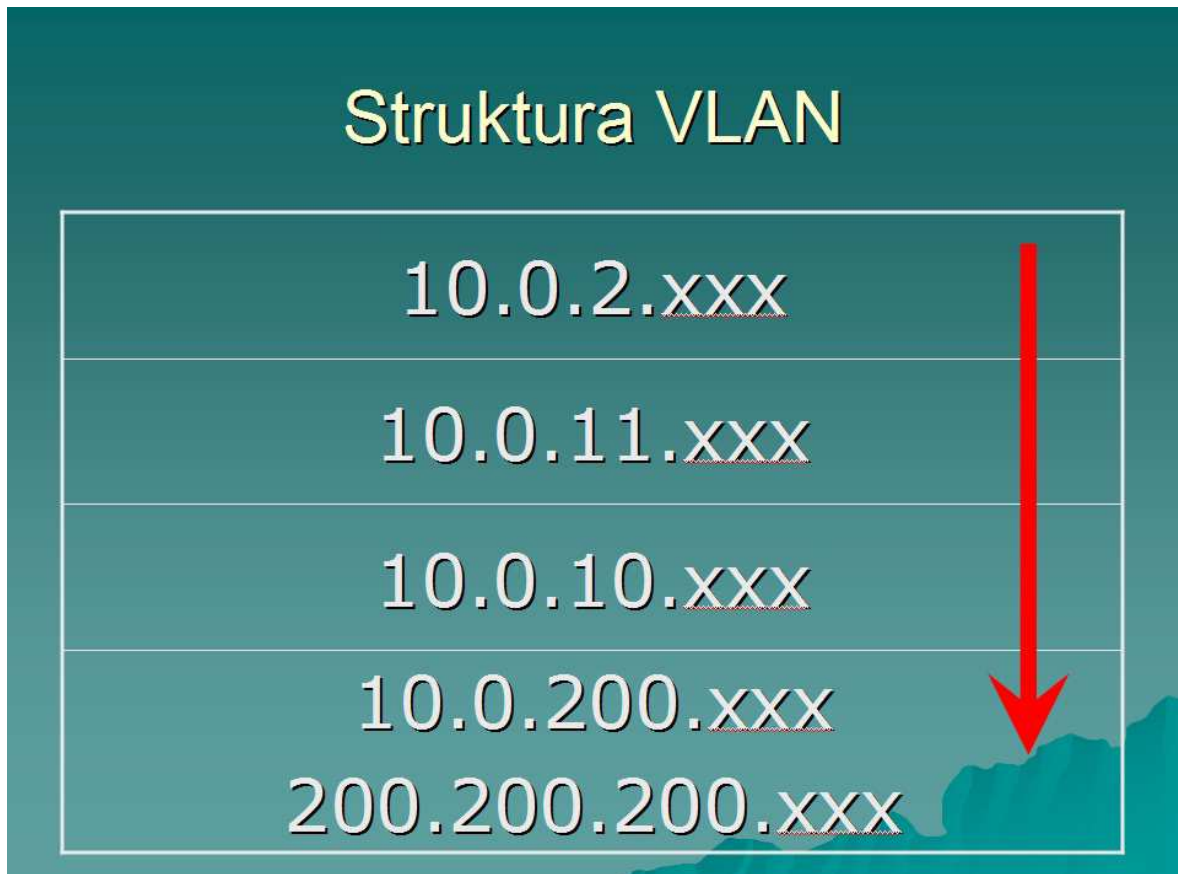
1. Hardwarovou – návrh a optimalizace struktury VLAN, propustnost a filtrování provozu nemocničního informačního systému.
2. Softwarovou – vytvoření detailního seznamu IP adres používaných v nemocničním informačním systému a zabránění připojení neznámých IP adres.
3. Aplikační – navrhnout a optimalizovat způsob přihlašování nových uživatelů a zoptimalizovat způsob přihlašování stávajících uživatelů nemocničního informačního systému.

## 6 NÁVRH A OPTIMALIZACE ZABEZPEČENÍ

### 6.1 Hardwarové zabezpečení

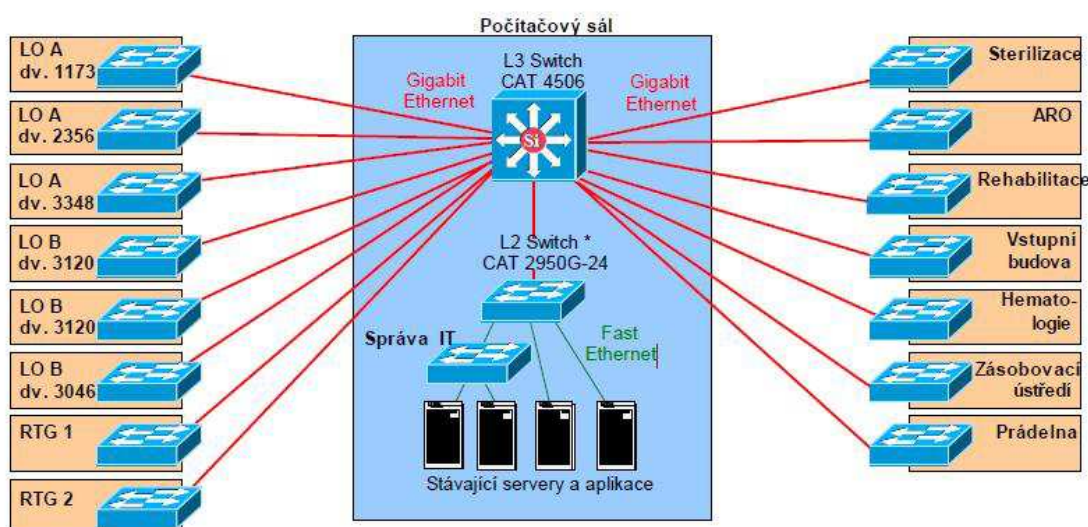
Nemocnice používala pouze dva rozsahy IP adres a to 200.200.200.2-254 a 10.0.200.2-254, které měli rovný přístup do celé sítě bez přesně stanovené bezpečnostní politiky. Toto nastavení umožňovalo neomezený přístup do celé sítě bez omezení. Hardwarové zabezpečení nemocničního informačního systému, které jsem zpracoval v rámci vypracovávané diplomové práce, je řešeno na úrovni protokolu TCP/IP a spočívá v systému nadřazených VLAN, ke kterým běžní uživatelé nemají přístup.

Touto změnou nastavení sítě došlo k významnému zvýšení bezpečnosti přístupu do sítě vytvořením systému nadřazených VLAN. Kde na nejvyšší úrovni je VLAN administrace aktivních prvků s maskou 10.0.2.X, které je podřazená VLAN administrátorů sítě s maskou 10.0.11.X. Nejnižší prioritu mají uživatelské VLAN s maskou 200.200.200.X a 10.0.200.X. Bohužel z historických důvodů je použita maska 200.200.200.X, která spadá do veřejných internetových adres, protože při budování sítě se nepředpokládalo, že by nemocniční datová síť byla někdy připojena jakýmkoliv způsobem do internetové sítě. Změna IP adres vzhledem k rozsáhlému použití jak v různém nastavení pravidel směrování laboratorních přístrojů, tak použití v laboratorních analyzátoch není bohužel možná (přístroje jsou nastaveny z výroby a není možná jejich konfigurace), ale nové zařízení se postupně nastavují do VLAN 10.0.200.X. V průběhu instalace byla vytvořena ještě VLAN ředitelství 10.0.10.X, která byla svými právy zařazena mezi uživatelskou a administrátorskou VLAN.



Obr. 16. Struktura VLAN

Topologie datové sítě je založena na nových optických vláknech, které spojují jednotlivé objekty (jednotlivé budovy areálu nemocnice) s datovým centrem (budova ředitelství počítačový sál). Na optických trasách je provozován Gigabit Ethernet s přenosovou rychlostí 1Gbps v plném duplexu. Topologie samotná je příkladem typické hvězdy, kdy na jeden centrální aktivní prvek jsou připojeny všechny části areálu nemocnice.



Obr. 17. Blokové schéma datové sítě

### 6.1.1 Centrální prvek

Jako centrální aktivní prvek je využíván přepínač Catalyst 4506 společnosti Cisco Systems. Přepínač je osazen výkonným řídicím modulem 4. generace s funkcionalitou přepínání na třetí vrstvě a bohatou podporou dalších funkcí jako je podpora kvality služby (QoS), filtrování provozu (ACL) a mnoho dalších nezbytných rysů pro budování podnikových sítí. Jednotka je osazena třemi moduly po 6-ti portech Gigabit Ethernetu, tzn. 18-ti pozicemi pro GBIC moduly. Tyto pozice jsou osazeny GBIC moduly. Počet těchto použitých GBIC modulů je 16, kdy 15 portů je použito pro připojované objekty a 1 port pro připojení stávající síťové infrastruktury (přepínač Cisco CAT 2950G-24).

### 6.1.2 Přístupové aktivní prvky

V jednotlivých objektech (přístupových bodech datové sítě) jsou nasazeny přepínače Cisco Catalyst 2950G a to buď s 24 porty nebo 48 porty 10/100Ethernetu (v závislosti na velikosti daného objektu). Dále je vybaven dvěma porty Gigabit Ethernetu, kdy fyzické připojení je realizováno opět prostřednictvím GBIC modulů. Pro připojení přístupového přepínače k centrálnímu přepínači je použit pouze jeden port. Na 10/100 Ethernet porty přepínače jsou připojeny převážně terminálové servery a pracovní stanice. Přepínače jsou dostatečně dimenzovány vzhledem k požadavku na přechod od znakových terminálů k osobním počítačům, tedy Ethernet připojení. Přepínače disponují dostatečným výkonem a podporou virtuálních sítí (VLAN) pro současné i budoucí využití.

### 6.1.3 IP adresace

Nemocnice využívá adresní prostor třídy C pro IP adresaci, konkrétně 200.200.200.0/24. Tato adresa sítě je v rozporu s RFC 1918, který definuje IP adresy využívané v Intranetech. Nicméně informační systém vznikl v době, kdy připojení nemocničních informačních systémů bylo zakázáno a v současné době změna na standardní masku není možná, protože převážná část především laboratorních analyzátorů připojených do nemocničního informačního systému neumožňuje změnu IP adresy (tyto jsou nastaveny z výroby). Přidělování IP adres v celé síti je prováděno manuálně bez použití DHCP. Na rozhraních (interface VLAN) centrálního přepínače/směrovače CAT 4506 jsou nasazeny rozšířené access-listy pro filtrování provozu v odchozím směru. Veškerý provoz, který není definován jako žádoucí je standardně blokován. Směrování IP provozu mezi logickými sítěmi (VLAN) zajišťuje centrální přepínač CAT 4506. Vzhledem k hvězdicové topologii sítě je prováděno směrování IP provozu automaticky (směrovač bez další konfigurace je schopen směrovat do přímo připojených sítí). Na směrovači je definován default-route směrem do Internetu (SQUID - IP adresa 200.200.200.9).

Konfiguraci VLAN na přístupových přepínačích lze rozdělit do tří částí:

- Definice parametrů VLAN – provádí se počáteční definice VLAN (identifikace, jméno). Ty jsou prováděny pouze na centrálním přepínači CAT 4506 a následně jsou šířeny přes VTP.
- Konfigurace VLAN Trunků – GigabitEthernet porty jsou definovány jako IEEE 802.1Q Trunk.
- Asociování přístupových portů k příslušné VLAN – je prováděno manuálně na 10/100 Ethernet portech přístupového přepínače. Port je přidělen do příslušné VLAN administrátorem sítě. 10/100 Ethernet porty přístupových přepínačů jsou převážně asociovány do VLAN 1 (z důvodu zpětné kompatibility). Výjimku tvoří pak uživatelé z VLAN 30 a VLAN 50, kteří jsou přiřazeni do odpovídající VLAN.

### 6.1.4 Uživatelská VLAN

Stávající zařízení sítě využívají adresového prostoru 200.200.200.0/24 a jejich konfigurace se nemění. Přesné adresové schéma dané logické sítě zůstává beze změny. V následujícím seznamu je uveden obecný přehled IP adresace.

Jméno systému	IP Adresa	Zařízení	Popis
RSw-C4506-Gate	200.200.200.1/24	CAT 4506	Default Gateway
Volný rozsah	200.200.200.4-254/24		Pro potřeby zařízení nemocnice

Stávajícím systémům jsou doplněny odpovídající default gateway, případně adresa WINS serveru pro zajištění kompletní funkčnosti daného zařízení v síti.

Tato logická síť je asociována s VLAN 1.

### 6.1.5 TOP management a finanční oddělení

VLAN TOP managementu a finančního oddělení je samostatná logická síť (10.0.10.0/24), která je využívána pracovníky TOP managementu a finančního oddělení. Samostatná logická síť je definována z důvodu lepšího prosazování bezpečnostní politiky – u uživatelů se nacházejí citlivá data.

Jméno systému	IP Adresa	Zařízení	Popis
RSw-C4506-Gate	10.0.10.1/24	CAT 4506	Default Gateway
Volný rozsah	10.0.10.4-254/24		Pro potřeby zařízení nemocnice

Stávajícím systémům je nutné doplnit odpovídající default gateway, případně adresu WINS pro zajištění kompletní funkčnosti daného zařízení v síti.

Tato logická síť je asociována s VLAN 30.

VLAN30-OUT, definice pravidel pro filtrování:

*permit ip host 200.200.200.4 any*

Povoluje přístup z MAIL Server.

*permit ip host 200.200.200.9 any*

Povoluje přístup z SQUID.

*permit ip host 200.200.200.40 any*

Povoluje přístup z HP UX.

*permit ip host 200.200.200.109 any*

Povoluje přístup z FreeServeru.

*permit ip 10.0.11.0 0.0.0.255 any*

Povoluje plný přístup z VLAN50 (ADMIN).

*deny ip 200.200.200.0 0.0.0.255 host 10.0.10.8*

Zamezuje přístup z VLAN 1 na PC.

*permit ip any host 10.0.10.8*

Povoluje plný přístup na INET pro PC.

*permit udp any any eq netbios-dgm*

*permit udp any any eq netbios-ns*

Povoluje 2 porty pro NETBIOS (NAME SERVICES).

### 6.1.6 Správa nemocničního informačního systému

VLAN správy nemocničního informačního systému je samostatná logická síť (10.0.11.0/24), která je využívána pracovníky správy a administrace IT. Samostatná logická síť je definována z důvodu lepšího prosazování bezpečnostní politiky – u uživatelé s privilegovaným přístupem (např. do logické sítě pro management aktivních prvků).

Jméno systému	IP Adresa	Zařízení	Popis
RSw-C4506-Gate	10.0.11.1/24	CAT 4506	Default Gateway
Volný rozsah	10.0.11.4-254/24		pro potřeby zařízení nemocnice

Stávajícím systémům je nutné doplnit odpovídající default gateway, případně adresu WINS pro zajištění kompletní funkčnosti daného zařízení v síti.

Tato logická síť je asociována s VLAN 50.

VLAN50-OUT, definice pravidel pro filtrování

*permit ip host 200.200.200.4 any*

Povoluje přístup z MAIL Server.

*permit ip host 200.200.200.9 any*

Povoluje přístup z SQUID.



*permit ip host 200.200.200.40 any*

Povoluje přístup z HP UX.

*permit ip host 200.200.200.109 any*

Povoluje přístup z FreeServeru.

*permit tcp 200.200.200.0 0.0.0.255 eq 2480 any*

Povoluje TELNET z Terminal Serveru.

*permit tcp 200.200.200.0 0.0.0.255 range 137 139 any*

Povoluje NETBIOS (mapování disku).

*permit tcp 200.200.200.0 0.0.0.255 any range 5800 5801*

*permit tcp 200.200.200.0 0.0.0.255 any range 5900 5901*

Povoluje VNC pro VLAN1.

*permit tcp 200.200.200.0 0.0.0.255 range 5800 5801 any*

*permit tcp 200.200.200.0 0.0.0.255 range 5900 5901 any*

Povoluje VNC pro VLAN1.

*permit ip 10.0.2.0 0.0.0.255 any*

Povoluje přístup z VLAN100 (NET-ADMIN).

*permit udp any any eq netbios-dgm*

*permit udp any any eq netbios-ns*

Povoluje 2 porty pro NETBIOS (NAME SERVICES).

*permit icmp any any*

Povoluje ICMP.

*deny ip 200.200.200.0 0.0.0.255 any*

Kompletní zakázání provozu z VLAN 1.

*permit ip any any*

Povoluje veškerý provoz.

### 6.1.7 Management aktivních prvků

VLAN managementu aktivních prvků je samostatná logická síť (10.0.2.0/24), která je využívána pro management aktivních prvků. Samostatná logická síť je definována z důvodu lepšího prosazování bezpečnostní politiky – zamezení přístupu neoprávněných uživatelských stanic v síti k managementu aktivních prvků.

Tato logická síť je asociována s VLAN 100.

Přiřazení pravidel k rozhraním

```
interface VLAN30
```

```
description TOP-MANAGEMENT
```

```
ip address 10.0.10.1 255.255.255.0
```

```
ip access-group VLAN30-OUT out
```

```
interface VLAN50
```

```
description ADMIN
```

```
ip address 10.0.11.1 255.255.255.0
```

```
ip access-group VLAN50-OUT out
```

```
interface VLAN100
```

```
description NET-ADMIN
```

```
ip address 10.0.2.1 255.255.255.0
```

```
ip access-group NET-ADMIN out
```

## 6.2 Softwarové zabezpečení

Dalším slabým místem je adresace připojení. Přepínače CISCO byly, jak jsem uvedl v kapitole hardwarového zabezpečení, nadefinovány pouze do jedné VLAN a všechny porty byly zapojeny a bylo možné se při zadání libovolné IP adresy v rozsahu 200.200.200.2-254 připojit na aplikační server. V rámci zpracování diplomové práce jsem vytvořil detailní soubor IP adres používaných v Nemocnici Břeclav NISstopology, která umožňuje přesnou identifikaci jak terminálů, tak PC zapojených do nemocničního informačního systému. Samozřejmostí je, že přístup do souboru NISstopology budou mít pouze administrátoři nemocničního informačního systému. Pokud zařízení s uvedenou IP adresou není v tomto souboru uloženo bude dané zařízení odmítnuto systémem a vypíše následující oznámení:

```
IP:(10.0.11.222) PC_Workstation_Xterminal Termttype:(unknown) LPrinter:(unknown)
```

```
Location:(unknown) ApplID:(unknown)
```

```
-----
```

Neznámý typ terminálu. Kontaktujte správce systému.

```
-----
```

logout

```
HP-UX hp-bv B.11.31 U ia64 (tSc)
login: batka
Password:
Last successful login: Tue May 7 10:53:07 METDST 2013 ja
Last authentication failure: Mon Mar 4 07:23:06 MET 2013 hp-bv
Please wait...checking for disk quotas
  Čekajte prosím (max. 30 sekund) ...
IP:(10.0.11.222) PC_Workstation_Xterminal Termttype:(unknown) LPrinter:(unknown)

Location:(unknown) ApplID:(unknown)
nnnnnnn
Neznámý typ terminálu. Kontaktujte správce systému.
nnnnnnn
logout

-----
Spojenie bolo ukoncene, znovu sa nadviaze po stlaceni klavesy ENTER...
-----
```

Obr. 18. Obrazovka terminálu s přihlášením neznámého pracoviště

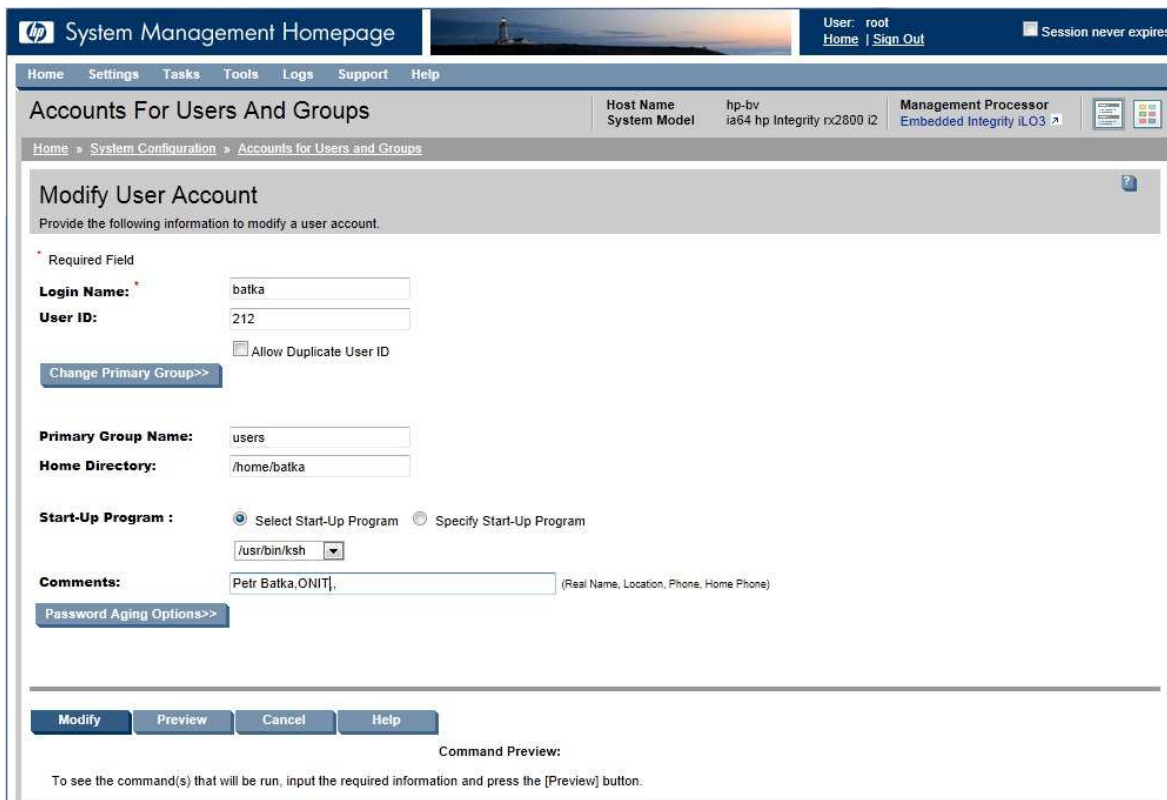
Uvedený postup je nastaven v domovském adresáři (/home/user) každého uživatele v souboru „profile“ a kontrolou příkazem „inet\_addr“ bude zjištěna IP adresa pracovní stanice. Dále soubor zajistí nemožnost spuštění příkazového řádku a uživateli se spustí přímo aplikace, která je dále zabezpečena v aplikační části. Tímto je zabezpečen neoprávněný přístup do nemocničního informačního systému.

```
[1] NISstopology-----14:33
10.0.200.150 00 emu lj41      CHIR_kolono         low;
10.0.200.151 00 EMU dj520    RTG_prim            low;
10.0.200.152 00 EMU lj41      RTG_VL_Dobias      low;
10.0.200.153 00 EMU lx300    RTG_DOK-wifi       low;
10.0.200.154 00 emu none     RTG_NAS             low;
10.0.200.155 00 emu none     NIS_konektor_A     low;
10.0.200.156 00 emu none     NIS_konektor_B     low;
10.0.200.157 00 EMU none     RTG_vedleKodaku    low;
10.0.200.158 00 EMU none     RTG_Kodak           low;
10.0.200.159 00 EMU dj520    RTG_dvere           low;
10.0.200.160 00 EMU none     RTG_okno            low;
10.0.200.161 00 EMU none     RTG_popis4         low;
10.0.200.162 00 EMU dj520    RTG_okno_Darmovz   low;
10.0.200.163 00 EMU none     RTG_CT_VZADU       low;
10.0.200.164 00 EMU none     RTG_CT_ovlad_vlevo low;
10.0.200.165 00 EMU none     RTG_ANGIO           low;
10.0.200.166 00 EMU lx300    RTG_evidence        low;
10.0.200.167 00 emu none     ARO_Vasicek        low;
10.0.200.168 00 emu lj41     REH_notas10000     low;
10.0.200.169 00 emu lx300    HEM_den_mistnost   low;
10.0.200.170 00 emu none     REH_telocvicna     low;
10.0.200.171 00 emu lx300    INF_AMB_ses        low;
+T::TTTTTTTTT:::T:::T:::T:::T:::T:::T:::T:::T:::
14 S 8:1 obn.^R OOT0 Mez Sloup Menu:F10
```

Obr. 19. Ukázka souboru NISstopology

### 6.3 Aplikační zabezpečení

Aplikační zabezpečení – každému uživateli nemocničního informačního systému je v aplikační části automaticky přiděleno uživatelské jméno, které se skládá z pěti písmen příjmení a tří písmen z křestního jména a sám si zadá heslo. Pro vkládání uživatelů se používá aplikační webové rozhraní na aplikačním serveru prostřednictvím https připojení a portu 2301.



The screenshot shows the HP System Management Homepage interface. The main content area is titled 'Accounts For Users And Groups' and contains a 'Modify User Account' form. The form includes the following fields and options:

- Login Name:** batka
- User ID:** 212
- Allow Duplicate User ID
- Change Primary Group>>** (button)
- Primary Group Name:** users
- Home Directory:** /home/batka
- Start-Up Program :**  Select Start-Up Program  Specify Start-Up Program
- Start-Up Program:** /usr/bin/ksh
- Comments:** Petr Batka, ONIT, (Real Name, Location, Phone, Home Phone)
- Password Aging Options>>** (button)

At the bottom of the form, there are buttons for 'Modify', 'Preview', 'Cancel', and 'Help'. Below these buttons is a 'Command Preview' section with the instruction: 'To see the command(s) that will be run, input the required information and press the [Preview] button.'

Obr. 20. Vložení nového uživatele

Administrátor nemocničního informačního systému zadává login (přihlašovací jméno) uživatele, systém poté přidělí ID uživatele. Dále se zadává uživatelská skupina, do které bude uživatel zařazen (users) a domovský adresář. Administrátor vybere startovací program a cestu k tomuto programu (/usr/bin/ksh). Posledním vyplňovaným polem je zapsání komentáře, do kterého vypisujeme celé jméno a pracoviště uživatele.

The screenshot displays the HP System Management Homepage interface for user administration. The main heading is "Accounts For Users And Groups". Below the heading, there are tabs for "Local Users", "Groups", and "User Templates". A search bar contains the text "batka". Below the search bar, a table lists the search results. The table has the following data:

Login Name	User ID	Primary Group	Real Name	Account Status
batka	212	users	Petr Batka	Enabled

Below the table, there is a message: "Select a user account in the list pane to view detailed information." The interface also includes a "Display: 50 Rows" dropdown menu and a "Printable View of Table" link.

Obr. 21. Administrace přístupových účtů

I po vložení mají možnost administrátoři nemocničního informačního systému měnit nastavení pro jednotlivé uživatele např. změnu skupiny nebo domovského adresáře. Často také dochází ke změně uživatelských hesel a to především z důvodů ztráty (zapomenutí) nebo v případě, že došlo k prozrazení přihlašovacích údajů. V aplikaci se provádí i mazání uživatelů při ukončení pracovního poměru.

Pomocí této aplikace je možno monitorovat činnost centrálního serveru a to jak v hardwarové, tak i softwarové úrovni. Je možné sledovat a upravovat nastavení serveru případně vytvářet systémové zálohy, které je možné exportovat např. na DAT pásky. Ve velké míře aplikaci používáme ke sledování chybových hlášení, které jsou ukládány do log souborů.

Data vytvořená v aplikaci při zakládání nového uživatele jsou uložena v klasické unixové struktuře v adresáři /etc v souboru passwd.

```

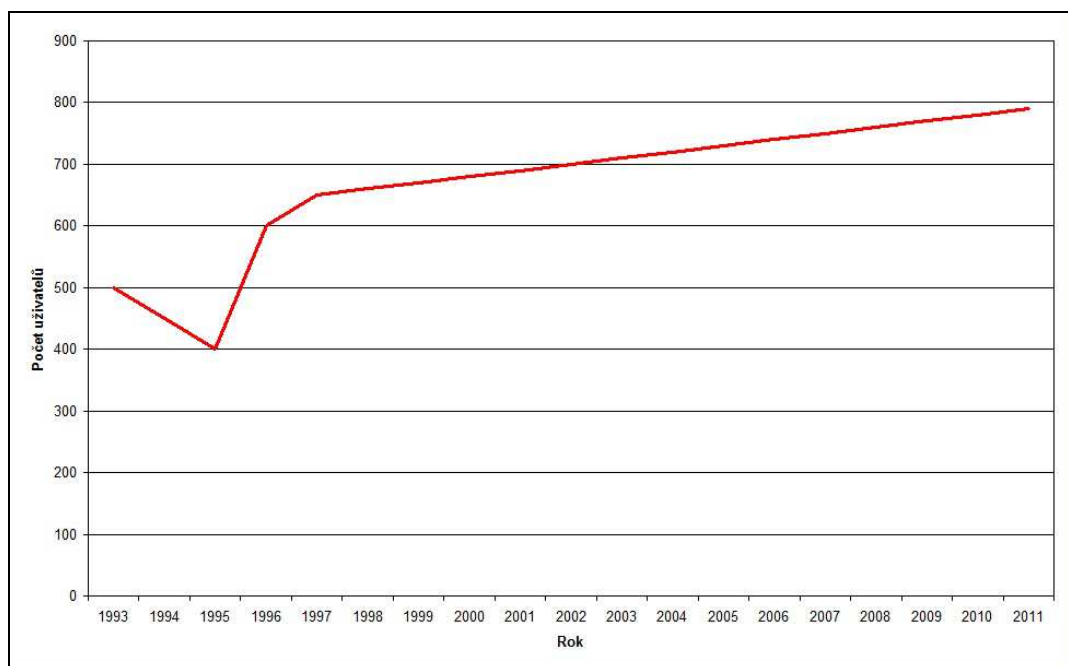
informix:v8nXw4CK162Kk:600:600::/opt/informix:/usr/bin/ksh
amis:NP4lr4iLNpzAA:6601:660::/AMIS_H/home/amis:/usr/bin/ksh
amisadm:iPqQ3JS6n8neU:6600:660::/AMIS_H/home/amisadm:/usr/bin/ksh
amisys:lQxCtLc3oVMPs:6602:660::/AMIS_H/home/amisys:/usr/bin/ksh
amitest:4FLsjn2ca.0es:6603:660:test.uzivatel:/AMIS_H/home/amitest:/usr/bin/ksh
batka:e5WonXmXCIInc:212:20:Petr Batka,JA,,:/home/batka:/usr/bin/ksh
erikac:pJoJboMR6.GW.:214:20:Cermakova Erika,Detske A,,:/home/erikac:/usr/bin/ksh
holca:d9Cg7PzX202UE:216:20:Holcapflova Ladislava,Detske A,,:/home/holca:/usr/bin/
/ksh
hrabalov:c7UQEPV.1ffjM:217:20:Hrabalova Gabina,Detske A,,:/home/hrabalov:/usr/bi
n/ksh
hrubaeva:azG2BwkW5AaSk:218:20:Hruba Eva,Detske A,,:/home/hrubaeva:/usr/bin/ksh
husakova:22kawQbKPF5Ed6:219:20:Husakova Vera,Detske A,,:/home/husakova:/usr/bin/k
sh
pavkova:40XPgfqvwmbNc:220:20:Pavkova Ilona,Zasobovani,,:/home/pavkova:/usr/bin/k
sh
jakoubko:bGxccrUCfBx1k:221:20:Jakoubkova Ruzena,Detske A,,:/home/jakoubko:/usr/b
in/ksh
jarosova:ccYsOkV2nTlz2:222:20:Jarosova Vera,Detske A,,:/home/jarosova:/usr/bin/k
sh
kucabova:9bRWk15dxy5DE:223:20:Kucabova Jana,Detske A,,:/home/kucabova:/usr/bin/k
sh
neuhaus*:224:20:Neuhauserova Jana,Detske A,,:/home/neuhaus:/usr/bin/ksh
novakova:yuVeb/HWUfFek:225:20:Novakova Alena,Detske A,,:/home/novakova:/usr/bin/
passwd (1%)

```

Obr. 22. Vzorek souboru passwd

Pro představu počtu uživatelů jsem vytvořil graf vývoje počtu uživatelů nemocničního informačního systému v Nemocnici Břeclav. Na následujícím grafu je jasně patrný nárůst počtu uživatelů nemocničního informačního systému.

Graf 2. Vývoj počtu uživatelů



Pokles v roce 1995 byl způsoben privatizací části hospodářsko – technického úseku (prádelna, stravovací provoz) a jejím převodem na jiné právnické subjekty. Naopak prudký nárůst uživatelů byl v roce 1996 způsoben otevřením II. etapy nemocnice (chirurgické obory).

### 6.3.1 Návrh a optimalizace aplikačního zabezpečení

Největší nebezpečí zabezpečení nemocničního informačního systému spočívá v zadávání hesel přímo uživateli a neměnnost hesla po celou dobu trvání pracovního poměru. Systém automaticky přiděluje uživatelské jméno (login) a to se skládá z pěti písmen z příjmení a tří písmen ze jména. Systém i v budoucnu bude automaticky přidělovat uživatelská jména, neboť tato skladba uživatelského jména se osvědčila a v podstatě nedochází k možnosti výskytu duplicit, kdy se musí uživatelské jméno přidělovat „ručně“. Co se týká přidělování hesel musí správa systému učinit radikální změnu a v první fázi „přinutit“ všechny uživatele ke změně hesla. Nově přichozím uživatelům již budeme přidělovat automaticky generované hesla v minimální konfiguraci 4 písmena z toho 1 velké a 4 číslice. Tímto předejdeme možnosti zadávání hesel typu : 1234, 0000, heslo atd. Nutno podotknout, že z uživatelského hlediska bude toto opatření podrobena velké kritice, protože většině uživatelů je pojem zabezpečení jejich vlastních přístupových údajů zcela lhostejné. Dále bude nastavena nutnost změny hesla každých 12 měsíců.

Rozsah přístupu zaměstnanců do jednotlivých subsystémů NIS je stanoven dle rozsahu činností, které vykonávají v rámci svých kompetencí a náplně práce. Dále je stanoven postup přidělení uživatelských práv k jednotlivým systémům a modulům nemocničního informačního systému.

Při uzavření pracovního poměru, po přidělení osobního čísla zaměstnanci jej pracovnice zaměstnaneckého oddělení zadá do nemocničního informačního systému a s vyplněným registračním formulářem odešle nově přijatého zaměstnance na oddělení nemocniční informatiky ONIT v den nástupu, nejpozději do 3 pracovních dnů od nástupu. Pracovníci oddělení nemocniční informatiky na základě registračního formuláře provedou přihlášení pracovníka v základním rozsahu dle oddělení na které nastupuje a pracovního zařazení.



```
AKCE: Hledej Další Předch Seznam Vlož Oprav Zruš Ukaž Návrat
Hledání položek do seznamu.
==(adm)==(batka)===== (1 / 1) ==
UŽIVATEL
-----
Login      : batka      Bc. BAŤKA PETR
Parametry :
-----
>Menu: adm          Název: Administrátor IS
   Poř: 1   Par:
>Menu: vyk_v2       Název: Výkaznictví
   Poř: 5   Par:
>Menu: poj          Název: POJIŠŤOVNA
   Poř: 7   Par: poj_cis
>Menu: oddeleni     Název: Oddělení
   Poř: 11  Par:
>Menu: ambulance    Název: Ambulance
   Poř: 14  Par:
>Menu: svls         Název: Agendy SVLS
   Poř: 16  Par:
-----
```

Obr. 23. Administrace přístupových práv

Vzhledem k nutnosti zajištění ochrany dat v souladu s platnou legislativou a z důvodu stanovení jednoznačného, pevného a prokazatelného postupu pro přidělování a rozšiřování uživatelských práv, jakož i jejich omezení jednotlivým uživatelům NIS, s cílem zamezení vzniku nedovoleného přístupu a případných následných škod z tohoto kroku plynoucích, jednotlivým zaměstnancům rozšíření nebo omezení přístupových práv do NIS umožněno pouze na základě registračního formuláře“, který bude dále sloužit pro zpřehlednění a zpětnou kontrolu v provozní oblasti NIS.

**Registrační formulář**

1. uživatel / žadatel	
Jméno	
Příjmení, titl.	
Osobní číslo	
Login	<small>(je-li již přidělen, event. doplní ONI)</small>
Oddělení	

2. žádám o přidělení těchto práv	
Oprávnění	* <input type="checkbox"/> primář <input type="checkbox"/> VS <input type="checkbox"/> lékař <input type="checkbox"/> dokumentátorka <input type="checkbox"/> sestra <input type="checkbox"/> jiný
Oddělení	

V případě uzavření pracovního poměru (nástupu po MD):

Pracovník ZO \_\_\_\_\_ podpis \_\_\_\_\_ datum \_\_\_\_\_

3. žádám o zrušení těchto práv	
Oprávnění	* <input type="checkbox"/> primář <input type="checkbox"/> VS <input type="checkbox"/> lékař <input type="checkbox"/> dokumentátorka <input type="checkbox"/> sestra <input type="checkbox"/> jiný
Oddělení	

**S přidělením / zrušením\*\* práv danému uživateli souhlasím.**

Nadřízený pracovník \_\_\_\_\_ podpis \_\_\_\_\_ datum \_\_\_\_\_

Vedoucí pracovník odd. \_\_\_\_\_ podpis \_\_\_\_\_ datum \_\_\_\_\_

**Souhlas primáře, vedoucího pracovníka jiného oddělení, než kterého je žadatel příslušníkem, příp. statutárního zástupce:**

Jméno: \_\_\_\_\_ podpis \_\_\_\_\_ datum \_\_\_\_\_

Datum: \_\_\_\_\_ podpis žadatele o změnu \_\_\_\_\_

Vyplní zaměstnanec ONI (administrátor AMIS\*H)

Požadované změny provedeny v rozsahu:.....

Jméno:..... podpis ..... datum.....

\* označit; \*\* nehodící se škrtněte

Obr. 24. Registrační formulář

Vlastní proces přihlášení nového uživatele, změna nebo omezení přístupových práv se realizuje na základě vyplněného formuláře s platným podpisem oprávněných osob. V případě změny přístupových práv zdravotnických pracovníků nelékařských oborů bude schvalovacím orgánem a oprávněnou osobou vrchní sestra daného oddělení. V případě lékařů a VŠ pracovníků primář, vedoucí pracovník oddělení. V případě potřeby rozšíření přístupových práv zaměstnance (konzilia, výpomoc na jiném oddělení atd.) na jiné pracoviště, než na které je zařazen, musí být na registračním formuláři rovněž schvalující podpis primáře, vedoucího pracovníka tohoto jiného oddělení. V případě žadatelů nezdravotnického personálu, je pro příslušnou oblast v rozsahu jejich funkčního zařazení a pracovní náplně, oprávněnou osobou a schvalovacím orgánem pro přístupová práva nadřízený pracovník žadatele. V případě přístupových práv nezdravotnického personálu ke zdravotnické dokumentaci, pokud její zpracování není v pracovní náplni pracovníka, podléhá toto schválení statutárním orgánem nemocnice. Výše uvedené postupy platí i pro případ omezení přístupových práv uživatelů. Zrušení přístupových práv se realizuje při ukončení pracovního poměru, nástupu na mateřskou dovolenou stejně na základě registračního formuláře.

Účelem dokumentu je stanovit dokumentovaný postup – pravidla pro zajištění bezpečnosti informací vč. integrity dat na pracovištích Nemocnice Břeclav, příspěvkové organizace a ochranu osobních údajů pacientů v souladu s platnou legislativou, zejména zákonem č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů.

Problematika, která je zpracována v této diplomové práci zajišťuje základní aplikační bezpečnostní postupy, které zajišťují:

1. Vypracování a uplatňování bezpečnostních postupů, které povolují pouze oprávněným osobám získat přístup k datům a informacím.
2. Přístup k různým kategoriím informací závisí na potřebnosti a je definován podle pracovního zařazení a funkce vč. studentů na výukových pracovištích.
3. Zavedení a udržování účinných procesů, které určují:
  - a) kdo má přístup k informacím;
  - b) informace, ke kterým má jednotlivec přístup;

- c) závazek uživatele pracovat s informacemi jako s důvěrnými;
  - d) postup pro narušení ochrany a zabezpečení.
4. Se zřetelem na zachování bezpečnosti informací o pacientech je určeno, kdo je oprávněn získat zdravotnickou dokumentaci pacienta a provádět v ní zápisy.
  5. Je stanoveno oprávnění osob, obsahu a formy zápisu v dané dokumentaci.
  6. Je zaveden postup, který zajišťuje, že pouze oprávněné osoby provádějí zápisy do zdravotnické dokumentace pacientů.

Veškeré informace, které jsou uloženy v nemocničním informačním systému, týkající se pacientů v jakékoliv formě jsou v organizaci považovány za důvěrné a musí s nimi jako s důvěrnými být nakládáno. Použití těchto informací při dalším zpracování je omezeno, jsou zpracovávány v rozsahu nezbytně nutném pro zajištění požadovaného nebo stanoveného výstupu, činnosti. Tam kde to lze, jsou informace zpracovávány formou anonymního údaje. Povinnost zaměstnanců o zachování mlčenlivosti a ochrany dat před zneužitím, odcizením a ztrátou je stanoveno v pracovním řádu v rozsahu dle funkčního zařazení, stanovených odpovědností a náplní práce.

## ZÁVĚR

Stávající používaný nemocniční informační systém AMIS\*H nepatří mezi nejmodernější informační systémy a je poplatný době svého vzniku, nicméně na českém trhu není zatím k dispozici žádný jiný nemocniční informační systém, který by dokázal tak komplexní informační systém nahradit. „Nedostatek“ grafického rozhraní je kompenzován instalací grafických rozšíření, které čerpají data přímo z databáze a slouží například k tisku sestav, případně graficky zobrazených trendů vývoje.

Veškeré úkoly, které jsem si dal za úkol zpracovat v diplomové práci jsem splnil a došlo k výraznému pokroku v komplexním zabezpečení nemocničního informačního systému v Nemocnici Břeclav. Výsledky SWOT analýzy mi umožnil relevantně stanovit oblasti zranitelnosti používaného nemocničního informačního systému AMIS\*H v Nemocnici Břeclav. Zranitelnost se ve své podstatě stala základem pro implementaci zásad zabezpečení ve vztahu k vybraným rizikům a zmiňovanou skutečnost lze vnímat i jako naplnění bodu zadání aplikování bezpečnostních zásad do nemocničního informačního systému. Navrhl jsem a optimalizoval zabezpečení nemocničního informačního systému ve třech oblastech na hardwarové, softwarové a aplikační úrovni. Na závěr můžu konstatovat, že při použití odpovídajících bezpečnostních programových prvků je nutné pro zabezpečení nemocničního informačního systému neustále průběžně zkoumat další možné bezpečnostní hrozby a to jak vnější, tak vnitřní hrozby, analyzovat tyto hrozby a následně učinit vhodná bezpečnostní opatření.

V případě, že bude na trhu s bezpečnostními informačními technologiemi dostupné kvalitnější řešení zajišťující vyšší míru zabezpečení, navrhuji jeho implementaci do nemocničního informačního systému. Současný vývoj a dostupnost internetových technologií a služeb představuje potencionální hrozbu pro všechny provozovatele a uživatele informačních systémů. Předpokládám, že by se průběžnou modernizací stávajícího nemocničního informačního systému předešlo možným budoucím bezpečnostním hrozbám.

## ZÁVĚR V ANGLIČTINĚ

Used existing hospital information system AMIS\*H is not among the most advanced information systems and is a product of its time, but the Czech market is not yet available to any other hospital information system that could and comprehensive information system to replace. "Lack of" graphical interface is compensated by installing graphics extensions that draw data directly from the database, for example to print reports or graphically displayed trends. Any task that I set myself the task process in my work I met a significant progress in comprehensive security hospital information systems in hospitals Breclav. The results of SWOT analysis allowed me to identify areas of vulnerability relevantly used hospital information system AMIS\*H Hospital Breclav. The vulnerability is essentially the basis for the implementation of security policies in relation to selected risk and these elements can also be seen as a fulfillment of terms of reference applying security policies to the hospital information system. I designed and optimized security hospital information system in three areas of the hardware, software and application level. In conclusion, I can say that the application of appropriate security program elements is necessary for security hospital information system constantly kept explore other possible security threats, both external and internal threats, analyze the threats and then take appropriate precautions. In the event that the market for information security technologies available to better solutions for higher level of security, I propose the implementation of a hospital information system. Current development and availability of Internet technology and services is a potential threat to all operators and users of information systems. I assume that the ongoing modernization of the existing hospital information system avoid possible future security threats.

**SEZNAM POUŽITÉ LITERATURY**

- [1] HANÁČEK, Petr a Jan STAUDEK. *Bezpečnost informačních systémů: metodická příručka zabezpečování produktů a systémů budovaných na bázi informačních technologií*. Praha: Úřad pro státní informační systém, 2000, 127 s. ISBN 80-238-5400-3.
- [2] JAŠEK R., *Závislost prosperity firmy na bezpečnosti informací*, 2005. 62 s.
- [3] KASAL, P. *Lékařská informatika*. Vyd. 1. Praha: Karolinum, 1998, 543 s. ISBN 80-718-4594-9.
- [4] *Průvodce zabezpečením pro malé organizace*. Microsoft Corporation, 2004. 51 s.
- [5] Zákon č. 372/2011 o zdravotních službách a podmínkách jejich poskytování. In: *131/2011*. 2011.
- [6] Zákon č. 101/2000 o ochraně osobních údajů a o změně některých zákonů. In: *32/2000*. 2000.
- [7] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. Vyd. 1. Brno: Computer Press, 2004, 190 s. ISBN 80-251-0106-1.
- [8] NORTH CUTT, S. *Bezpečnost sítí*. Vyd. 1. Brno: Computer Press, 2005, 589 s. ISBN 80-251-0697-7.
- [9] TVRDÍKOVÁ, M. *Zavádění a inovace informačních systémů ve firmách*. 1. vyd. Praha: Grada, 2000, 110 s. ISBN 80-716-9703-6.
- [10] VRANA, I. *Zásady a postupy zavádění podnikových informačních systémů*. 1. vyd. Praha: Grada, 2005, 187 s. ISBN 80-247-1103-6.
- [11] BERGER, Josef. *Informatika v klinické praxi pro lékaře a klinické biology*. Praha: Grada, 1993, 418 p. ISBN 80-856-2378-1.
- [12] LOCKHART, A. *Bezpečnost sítí na maximum*. Vyd. 1. Brno: Computer Press, 2005, 276 s. ISBN 80-251-0805-8.
- [13] *Informační systémy ve zdravotnictví*. České Budějovice, 2007. Skripta. Jihočeská univerzita v Českých Budějovicích, Zdravotně sociální fakulta.

- [14] *Česká společnost zdravotnické informatiky a vědeckých informací* [online]. 2013 [cit. 2013-04-13]. Dostupné z: <http://www.medinfo.cz/>
- [15] *ICZ a. s.: Integrovaná softwarová a síťová řešení* [online]. 2013 [cit. 2013-04-13]. Dostupné z: <http://www.icz.cz/co-delame/zdravotnictvi/>
- [16] *STAPRO s. r. o.: Komplexní řešení pro zdravotnictví* [online]. 2013 [cit. 2013-04-13]. Dostupné z: <http://www.stapro.cz/>
- [17] *CompuGroup Medical Česká republika s.r.o.: Spojujeme zdravotnictví* [online]. 2013 [cit. 2013-04-13]. Dostupné z: <http://www.cgm.cz/>
- [18] *IZIP: Elektronická zdravotní knížka* [online]. 2013 [cit. 2013-04-13]. Dostupné z: <http://www.izip.cz/>
- [19] *Ústav zdravotnických informací a statistiky ČR* [online]. 2013 [cit. 2013-04-13]. Dostupné z: <http://www.uzis.cz/>
- [20] ZVÁROVÁ, J. *Biomedicínská informatika: Základy informatiky pro biomedicínu a zdravotnictví*. 1. vyd. Praha: Karolinum, 2002, 162 s. ISBN 80-246-0609-7.
- [21] KASAL, P. *Internet a medicína*. 1. vyd. Praha: Grada, 2001, 224 s. ISBN 80-247-0119-7.



**SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK**

a. s.	Akciová společnost	
CT	Celotělový tomograf	
ČR	Česká republika	
ČSN	Česká státní norma	
	Dynamic Host Configuration	
DHCP	Protocol	
EN	Evropská norma	
HUB	Rozbočovač	
IP	Internet protokol	
ISO	International Organization for Standardization	Mezinárodní organizace pro tvorbu norem
IT	Informační technologie	
NIS	Nemocniční informační systém	
	Oddělení nemocniční	
ONIT	informatiky a telekomunikací	
p. o.	Příspěvková organizace	
	Picture Archiving and	Obrazový archivační a
PACS	Communicating System	komunikační systém
ROP	Regionální operační program	
s. r. o.	Společnost s ručením omezeným	
Sb.	Sbírka	
ÚZIS	Ústav zdravotnických informací a statistiky	
VLAN	Virtual Local Area Network	Virtuální lokální počítačová síť
VTP	VLAN Trunking Protocol	
VZP	Všeobecná zdravotní pojišťovna	

## SEZNAM OBRÁZKŮ

- Obr. 1. Modul lůžkového oddělení
- Obr. 2. Modul ambulance
- Obr. 3. Modul biochemické laboratoře
- Obr. 4. Blokované schéma toku dat [3]
- Obr. 5. Modul radiodiagnostického oddělení
- Obr. 6. Ukázka obrazových dat
- Obr. 7. Modul zdravotní pojišťovny pojišťovny
- Obr. 8. Modul účetnictví
- Obr. 9. Modul stravovacího provozu
- Obr. 10. Modul dopravní zdravotní služby
- Obr. 11. Modul správy systému
- Obr. 12. Server HP 9000 G40
- Obr. 13. Úvodní stránka nemocničního informačního systému AMIS\*H
- Obr. 14. HP Integrity server rx2800 i2
- Obr. 15. Přepínač CISCO CATALYST 4506
- Obr. 16. Struktura VLAN
- Obr. 17. Blokované schéma datové sítě
- Obr. 18. Obrazovka terminálu s přihlášením neznámého pracoviště
- Obr. 19. Ukázka souboru NISstopology
- Obr. 20. Vložení nového uživatele
- Obr. 21. Administrace přístupových účtů
- Obr. 22. Vzorek souboru passwd
- Obr. 23. Administrace přístupových práv
- Obr. 24. Registrační formulář

## SEZNAM TABULEK A GRAFŮ

Graf 1. Vývoj počtu instalovaných systémů v ČR

Graf 2. Vývoj počtu uživatelů