VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

ÚSTAV SOUDNÍHO INŽENÝRSTVÍ

INSTITUTE OF FORENSIC ENGINEERING

POSOUZENÍ INFORMAČNÍHO SYSTÉMU FIRMY A NÁVRH ZMĚN

INFORMATION SYSTEM ASSESSMENT AND PROPOSAL FOR ICT MODIFICATION

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — Bc. MICHAL ČERNOHORSKÝ
AUTHOR

VEDOUCÍ PRÁCE — doc. Ing. MILOŠ KOCH, CSc.
SUPERVISOR

BRNO 2014

Vysoké učení technické v Brně, Ústav soudního inženýrství

Ústav soudního inženýrství
Akademický rok: 2013/2014

ZADÁNÍ DIPLOMOVÉ PRÁCE

student(ka): Bc. Michal Černohorský

který/která studuje v **magisterském navazujícím studijním programu**

obor: **Řízení rizik firem a institucí (3901T048)**

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách a se Studijním a zkušebním řádem VUT v Brně určuje následující téma diplomové práce:

Posouzení informačního systému firmy a návrh změn

v anglickém jazyce:

Information System Assessment and Proposal for ICT Modification

Stručná charakteristika problematiky úkolu:

Úvod
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza problému
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Cíle diplomové práce:

Analyzovat stávající stav informačního systému vybrané organizace a jeho efektivnosti, posoudit tento stav a navrhnout změny, směřující ke zlepšení stávajícího stavu a eliminaci nalezených rizik.

Seznam odborné literatury:

BASL, Josef; BLAŽÍČEK, Roman. Podnikové informační systémy: Podnik v informační společnosti. 2. výrazně přepracované a rozšířené vydání. Praha : Grada Publishing, 2000. 283 s. ISBN 978-80-247-2279-5.
DOSTÁL, Petr; RAIS, Karel; SOJKA, Zdeněk. Pokročilé metody manažerského rozhodování. 1. vydání. Praha : Grada Publishing, 2005. 168 s. ISBN 80-247-1338-1.
MOLNÁR, Zdeněk. Efektivnost informačních systémů. 1. vydání. Praha : Grada Publishing, 2000. 144 s. ISBN 80-7169-410-X.
ŘEPA, Václav. Podnikové procesy : Procesní řízení a modelování. 2. aktualizované a rozšířené vydání. Praha : Grada Publishing, 2007. 288 s. ISBN 978-80-247-2252-8.
SODOMKA, Petr. Informační systémy v podnikové praxi. 1. vydání. Brno : Computer Press, a.s., 2006. 351 s. ISBN 80-251-1200-4.

Vedoucí diplomové práce: doc. Ing. Miloš Koch, CSc.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2013/2014.

V Brně, dne 10.9.2013

L.S.

doc. Ing. Aleš Vémola, Ph.D.
Ředitel vysokoškolského ústavu

Abstrakt

Tato diplomová práce se zabývá posouzením informačního systému organizace. Práce je rozdělena na dvě části. První se věnuje teoretickému popisu informačních systémů a definici rizika. Druhá část se věnuje cíli práce, tedy analýze stávající stavu informačního systému organizace, identifikaci rizik a návrhu změn, směrujících ke zlepšení stávajícího stavu a eliminaci nalezených rizik.

Abstract

This diploma thesis deals with assessment of the organization's information system. This work is divided into two parts. The first part addresses theoretical description of the information systems and the definition of risks. The second part addresses the objectives of this work, which is the analysis of the current condition of the organization’s information system, identification of risks and suggestions of changes that aims to improve the current state of system and to eliminate discovered risks.

Klíčová slova

Informační systém, riziko, HOS 8, efektivnost.

Keywords

Information system, risk, HOS 8, efficiency.

Bibliografická citace mé práce:

ČERNOHORSKÝ, M. *Posouzení informačního systému firmy a návrh změn.* Brno: Vysoké učení technické v Brně, Ústav soudního inženýrství, 2014. 75 s. Vedoucí diplomové práce doc. Ing. Miloš Koch, CSc..

Prohlášení

Prohlašuji, že jsem diplomovou práci zpracoval samostatně a že jsem uvedl všechny použité informační zdroje.

V Brně dne ……

…….

Michal Černohorský

Poděkování

Na tomto místě bych chtěl poděkovat vedoucímu diplomové práce doc. Ing. Miloši Kochovi, CSc., za cenné rady při vedení této diplomové práce a umožnění použití otázek pro posouzení systému na portálu ZEFIS. Dále všem, kteří se podíleli na vzniku této práce a zejména zaměstnancům organizace, kteří poskytli i informace a vyplnili dotazníky.

OBSAH

ÚVOD A CÍL PRÁCE

Informační systémy se v poslední době velmi rozšířily. I tam, kde před 10 – 15 lety pracoval s počítačem jeden člověk, se dnes bez něj neobejde téměř nikdo. Za tuto dobu ale také vzrostla potřeba některých informací a požadavky na tyto informace. Informační systémy se tak staly nedílnou součástí běžného pracovního dne pracovníků ve všech podnicích i organizacích. Tyto systémy, které se používají, by měly především zjednodušit a zefektivnit každodenní práci zaměstnanců. IS není jen hardware a software, ale především musí lidem v jejich práci pomáhat a ne být spíše na obtíž. Teprve poté můžeme hovořit o zefektivňování lidské práce. Je také nutné, aby pokud možno IS příliš nezastarával. Měly by tedy být rozvíjeny jeho možnosti podle aktuálních požadavků a měl by též zohledňovat změny v oblasti legislativy. Náležitou pozornost je poté i nutné věnovat zálohování a bezpečnosti informací, kdy dříve se citlivé informace daly pod zámek, ale nezabezpečený počítač obsahující tyto údaje pocit ohrožení nevzbuzuje.

Cílem práce je:

Analyzovat stávající stav informačního systému vybrané organizace a jeho efektivnost, posoudit tento stav a navrhnout změny směřující ke zlepšení stávajícího stavu a eliminaci nalezených rizik.

1 TEORETICKÁ VÝCHODISKA PRÁCE

1.1 ZÁKLADNÍ POJMY

Než začneme definovat informační systém, musíme si nejdříve objasnit, co jsou to data, informace a znalosti.

Data slouží pro reprezentaci faktů, atributů, odrazů dějů a věcí. Jsou tedy vyjádřením skutečností a myšlenek v podobě vhodné pro zpracovávání, uchovávání. Používají se zejména pro vytváření informací.

Informace - informace pochází z latinského slova *„informare“* = utvářet podobu, formovat. Pojem informace dodnes není jednoznačně vymezen. Definice závisí zejména na vědním oboru, ve kterém se používá[1].

„Informace je nový prvek v lidském poznání, které jedinec získává zpracováním dat, jež mají určitý konkrétní význam, takže jedinec je z informací schopen získat poznatky a znalosti.“[2]

„Informací může být vše, co zvyšuje poznatkovou úroveň jedince.“ [2]

Znalosti jsou na rozdíl od dat a informací charakteru nehmotného. Představují to, co člověk zná či umí a pomocí nichž je schopen vytvářet další informace. Tedy znalosti člověk potřebuje pro pochopení informací a z informací získává další znalosti.

Informace mohou být různě napadány. Může dojít k jejich narušení, poškození nebo změně. Tyto změny mohou být způsobeny úmyslně i neúmyslně a pro informační systém je tedy nutné zajišťovat jejich kvalitu. U informace tedy musíme dbát na to, aby byla spolehlivá (soulad informace s předlohou) a důvěryhodná (zabezpečení proti chybám a manipulacím). Kvalitu informace ovlivňují chyby (nesprávné operace provedené člověkem nebo strojem), šum (přídavná informace různé intenzity) nebo manipulace s informacemi (je lidského původu, někdy neúmyslná).[3]

---

[1] JANÍČEK, Přemysl a Jiří MAREK. Expertní inženýrství v systémovém pojetí. 1. vyd. Praha: Grada, 2013, 592 s. ISBN 978-80-247-4127-7., str. 54,55

[2] JANÍČEK, Přemysl a Jiří MAREK. Expertní inženýrství v systémovém pojetí. 1. vyd. Praha: Grada, 2013, 592 s. ISBN 978-80-247-4127-7., str. 55

[3] BÉBR, Richard a Jiří MAREK. Informační systémy pro podporu manažerské práce. 1. vyd. Praha: Professional Publishing, 2005, 592 s. Expert (Grada). ISBN 80-864-1979-7.str 31-35

Systém – v teorii systémů se systémem rozumí uspořádaná množina prvků, jejich vlastností a vazeb mezi nimi.

Informační systém – má opět celou řadu definic. Molnár definuje informační systém takto: „*Informační systém je soubor lidí, technických prostředků a metod (programů), zabezpečujících sběr, přenos, zpracování a uchování dat za účelem prezentace informací pro potřeby uživatelů činných v systémech řízení.*“ [4]

Informační technologie – „*lze chápat jako množinu prostředků a metod sloužících k práci s daty a informacemi.*“[5]

1.2 INFORMAČNÍ SYSTÉMY

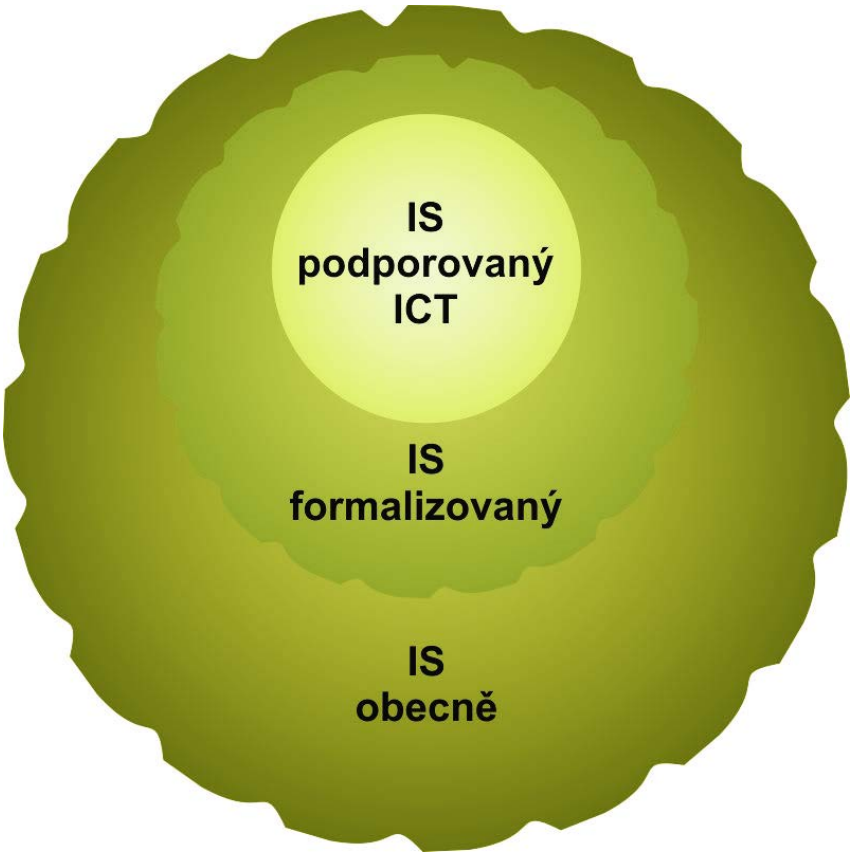
Informační systémy nejsou pouze v souvislosti s ICT, ale mohou být vnímány šířeji. To znamená, že do nich zahrneme i lidský faktor, formalizaci údajů nebo třeba nosiče informací. Proto je pro podporu inovací nutná následující trojice informací v rámci slupkového modelu.

- Informace zapsané a zpracované v databázích, které mají za úkol u určitých činností eliminovat přímou účast člověka, u jiných činností pomáhají člověku k rozhodnutí – jedná se o standartní podniková softwarová řešení
- Informace uložené na papírových dokladech, formulářích, předpisech a zprávách. Tyto informace jsou často nestrukturované (textový nebo grafický tvar) a jsou obtížněji dostupné.
- Informace, které nejsou nikde zaznamenány, tj. informace jako znalosti zaměstnanců, které používají operativně podle potřeb např. při rozhodování, projektování, výrobě,…[6]

[4] MOLNÁR, Zdeněk a Jiří MAREK. Efektivnost informačních systémů. 1.vyd. Praha: Grada Publishing, 2005, 142 s. Expert (Grada). ISBN 80-716-9410-X. str. 15

[5] VYMĚTAL, Dominik a Jiří MAREK. Informační systémy v podnicích: teorie a praxe projektování. 1. vyd. Praha: Grada, 2009, 142 s. Expert (Grada). ISBN 978-80-247-3046-2., str. 15

[6] BASL, Josef. *Inovace podnikových informačních systémů: podpora konkurenceschopnosti podniků*. 1. vyd. Praha: Professional Publishing, 2011, 150 s. ISBN 978-80-7431-045-4. str116, 117



Obrázek 1 – Roviny chápání IS v podniku

„Od těchto nosičů, jsou odvozeny tři roviny chápání informačního systému

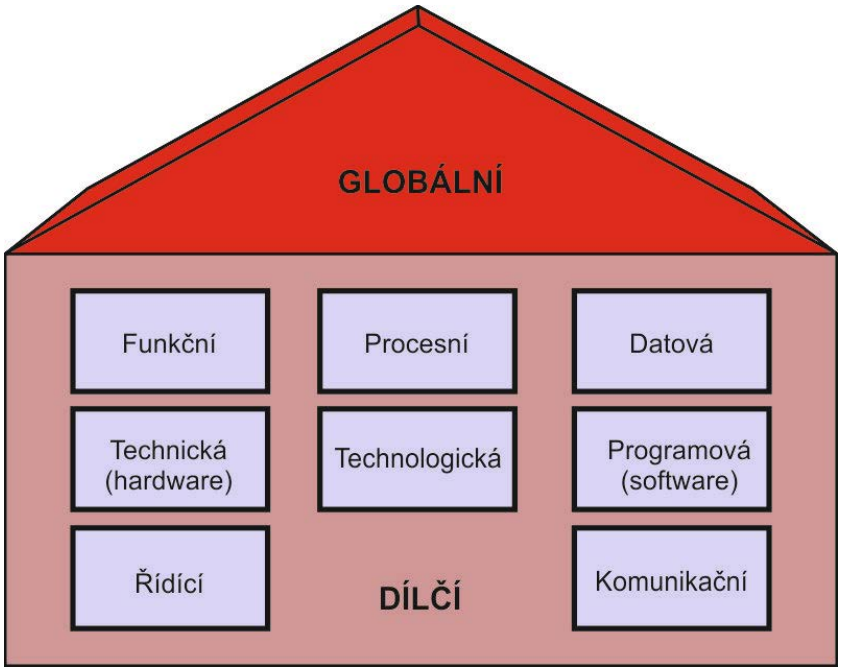
- *Informační systém podporovaný ICT,*
- *Informační systém formalizovaný,*
- *Obecně komplexní sociotechnický informační systém podniku.“*[7]

Ve všech těchto rovinách je postupný nárůst, který je nejvíce patrný v jejím jádru a části formalizovaného systému[7].

[7] BASL, Josef. *Inovace podnikových informačních systémů: podpora konkurenceschopnosti podniků*. 1. vyd. Praha: Professional Publishing, 2011, 150 s. ISBN 978-80-7431-045-4. str116, 117

1.2.1 Z pohledu architektur

Podstatou a účelem architektur je integrační tendence při vývoji IS/IT a rostoucí komplexnost systému, který má za úkol podporovat podnikové cíle. Tento integrovaný systém je složen z komponentů různých výrobců, které jsou spolu vzájemně propojeny a spolupracují. Systém má podpořit veškeré významné podnikové procesy.[8]



Obrázek 2 – IS z pohledu architektur [9]

Funkční architektura dělí IS na jednotlivé subsystémy nebo skupiny funkcí postupným rozdělováním globální architektury až na jednotlivé základní funkce.

Procesní architektura se zaměřuje na popis neautomatizovaných činností a funkcí IS a jejich reakcí na události, ke kterým může dojít. Jejím cílem je co nejefektivnější reakce podniku na externí události.

Technická architektura neboli hardwarová určuje typy a rozmístění prostředků výpočetní a komunikační techniky, vazby jednotlivých komponent. Je znázorněna schématem a specifikací počítačových sítí, serverů a počtem koncových PC a dalších zařízení[9]

[8] ŠMÍD, Vladimír. *Management informačního systému* Dostupné z: http://www.fi.muni.cz/~smid/mis-mdis.htm .

[9] KOCH, Miloš a Kol. Management informačních systémů. Vyd. 2., přeprac. Brno: Akademické nakladatelství CERM, 2010, 171 s. Učební texty vysokých škol. ISBN 978-80-214-4157-6, str.13.14, 15

Technologická architektura *„určuje způsob zpracování jednotlivých aplikací v návaznosti na technickou, datovou a programovou architekturu. Zahrnuje:*

- *Způsob zpracování aplikací*
- *Způsob zpracování dat*
- *Vnitřní stavbu aplikací*
- *Uživatelské rozhraní aplikací“* [10]

Datová architektura je návrhem datové základny podniku. Při jejím návrhu se vychází z jednotlivých objektů, jejich položek a vazeb mezi nimi, databázových tabulek a jejich fyzického uložení.

Programová architektura neboli softwarová určuje z jakého softwaru a jeho komponent se bude IS skládat a jaké vazby mezi nimi budou.

Komunikační architektura určuje vnější rozhraní systému a způsob jeho komunikace s okolím.

Řídící architektura *„určuje pravidla fungování systému, organizaci služeb uživatelům, standarty a organizační strukturu.“*[10]

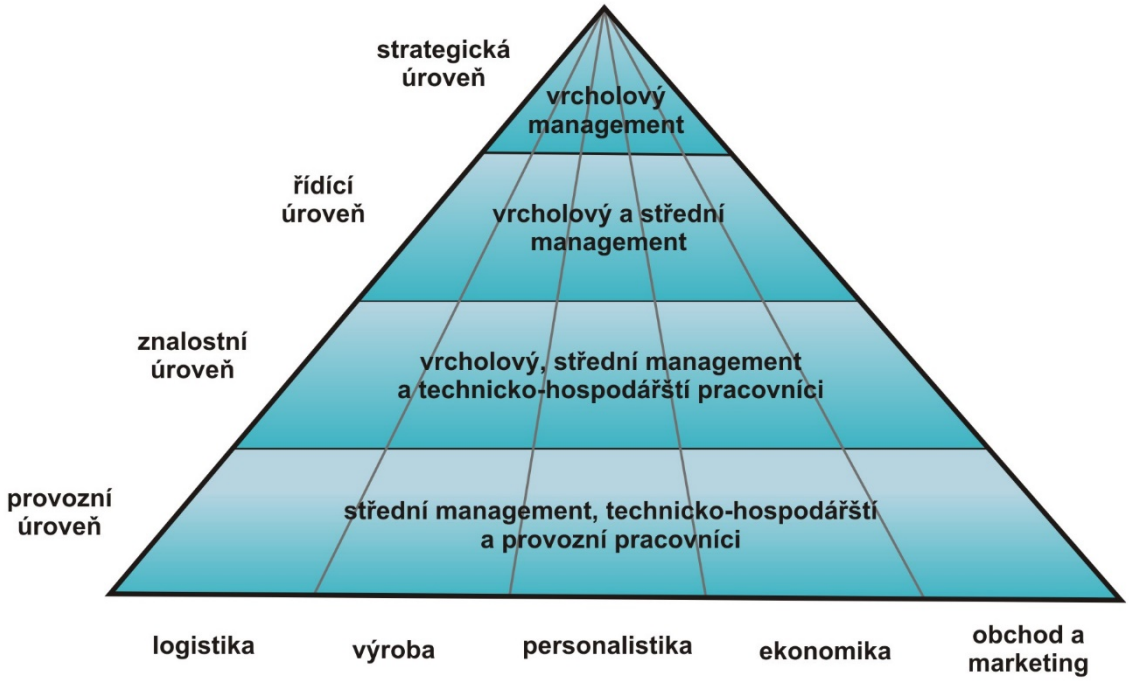
Globální architektura by měla být vizí budoucího stavu IS/IT. *„Tvoří ji jednotlivé stavební bloky, které představují skupiny aplikací včetně jejich datových základen a technického vybavení. Výše zmíněné dílčí architektury se pak zaměřují na podrobnější návrhy IS podle různých hledisek.“*[10]

Kromě návrhu jednotlivých stavebních bloků zahrnuje globální architektura i hrubý návrh vazeb mezi stavebními bloky. Tyto vazby musí být respektovány, ať je stavební blok řešen jakýmkoli softwarem.[10]

[10] VOŘÍŠEK, Jiří. Strategické řízení informačního systému a systémová integrace. Vyd. 1. Praha: Management Press, 2006, 323 s. ISBN 80-859-4340-9, str. 157

1.2.2 Z pohledu úrovně řízení

V každé organizaci je několik úrovní, kde každá požaduje svůj vlastní způsob zpracování informací, popřípadě i jejich druh.



Obrázek 3 – IS z pohledu úrovně řízení [11]

Provozní úroveň – tato úroveň v organizaci požaduje zpracování informací týkajících se běžné podnikové agendy, jako je realizace nákupu a prodeje, stejně tak výplat. Systémy v této úrovni reagují na plnění každodenních činností, musí poskytovat přesné, aktuální a snadno dostupné informace. Typickým zástupcem, který užívá tyto informace, je účetní nebo provozní pracovník.

Znalostní úroveň – tato úroveň zahrnuje kromě klientské části informačního systému, jako je ERP, CRM, atd. také prostředky tzv. osobní informatiky, jako jsou[11]:

- *Textový editor,*
- *Tabulkový procesor,*
- *Prezentační program pro tvorbu obrázků, schémat a prezentací,*

[11] SODOMKA, Petr. Informační systémy v podnikové praxi. Vyd. 1. Brno: Computer Press, 2006, 351 s. ISBN 80-251-1200-4, str. 72-73

- *Snímání papírových dokumentů a rozpoznávání jejich textu,*
- *Plánovací kalendář,*
- *Sledování úkolů,*
- *Elektronická pošta,*
- *Evidence pošty,*
- *Videokonference,*
- *Archiv dokumentů,…*[12]

tyto aplikace tedy slouží k růstu znalostní báze organizace a řídí tok dokumentů. Na jejich základě se rozvíjí i zkušenosti pracovníků. Uživateli těchto aplikací jsou technicko–hospodářští pracovníci na všech úrovních a manažeři.

Řídící úroveň – vyžaduje informace k plnění různých administrativních úkolů a slouží k podpoře rozhodování středního a vrcholového managementu. Informační systém této úrovně poskytuje odpovědi na zásadní otázku, zda věci fungují tak, jak mají. Tyto odpovědi poté poskytuje většinou formou reportingu, což jsou vygenerované výstupní sestavy, které obsahují souhrny výsledků z požadované oblasti.

Strategická úroveň – informační systémy této oblasti pomáhají vrcholovému managementu k určení dlouhodobých trendů jak uvnitř, tak i vně organizace. Jejich úkolem je pomáhat odhalovat očekávané změny a určovat jak a jestli je podnik schopen na změnu reagovat. Informace pro analýzy pocházení většinou z vnitřních zdrojů, to je z provozního systému organizace.[13]

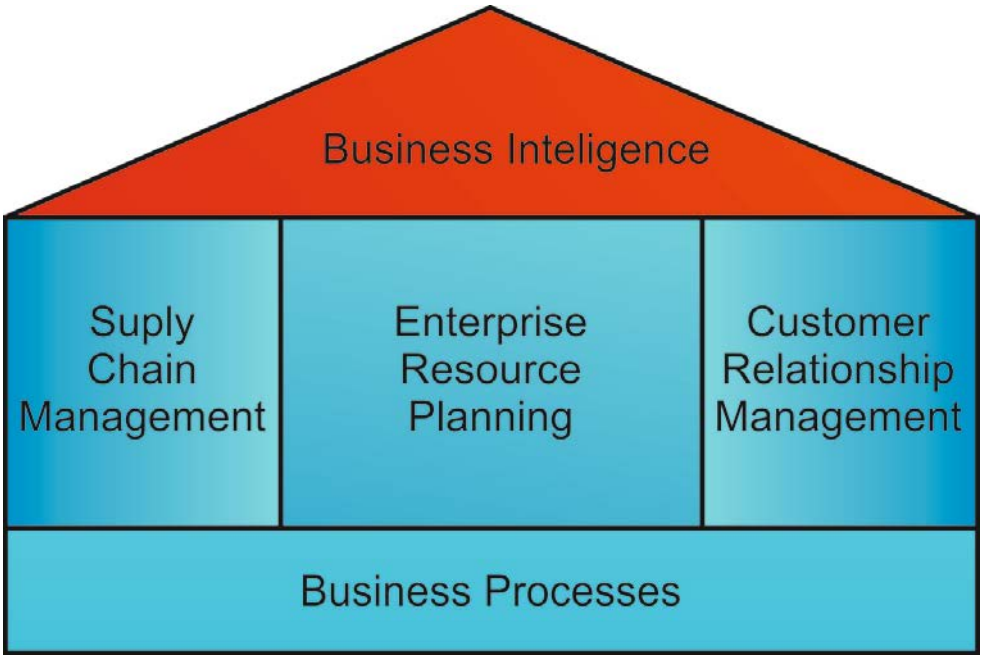
[12] VOŘÍŠEK, Jiří. Strategické řízení informačního systému a systémová integrace. Vyd. 1. Praha: Management Press, 2006, 323 s. ISBN 80-859-4340-9, str. 157

[13] SODOMKA, Petr. Informační systémy v podnikové praxi. Vyd. 1. Brno: Computer Press, 2006, 351 s. ISBN 80-251-1200-4, str. 73-74

1.2.3 Holisticko-procesní pohled

Podle této klasifikace je IS složen z:

- ERP – (Enterprise Resourcing Planning) hlavní část zaměřená na řízení interních podnikových procesů
- CRM – (Customer Relationship management)je zaměřen na řízení procesů týkajících se zákazníků
- SCM – (Supply Chain Management) řídí procesy zaměřené na dodavatele. Většinou je jeho součástí část APS (pokročilé plánování a rozvrhování výroby)
- BI – (Business Intelligence – Podnikové zpravodajství), též manažerský informační systém, funguje podobně jako v předchozí kapitole. Sbírá data z jednotlivých výše zmíněních částí a z externích zdrojů. Poskytuje informace pro rozhodování.[14]



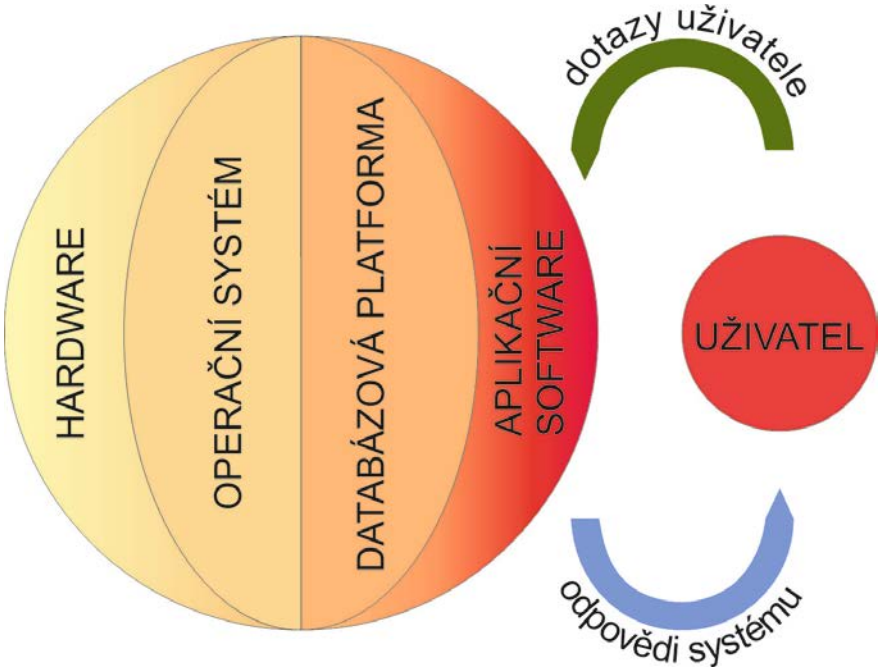
Obrázek 4 – holisticko-procesní pohled na IS[14]

[14] SODOMKA, Petr. Informační systémy v podnikové praxi. Vyd. 1. Brno: Computer Press, 2006, 351 s. ISBN 80-251-1200-4, str. 77-78

1.2.4 Technologický pohled na IS

Jedná se o třídění na jednotlivé části, přes které jsou data měněna na informace srozumitelné uživateli. Existuje mnoho vlivů, které specifikují, jak probíhá zpracovávání dat informačním systémem. Proto platí:

„nedílnou součástí podnikového informačního systému je hardwarová a softwarová infrastruktura, která podmiňuje efektivní automatizované zpracovávání dat prostřednictvím softwarových aplikací do interpretovatelné a srozumitelné podoby."[15]



Obrázek 5 – technologické pojetí informačního systému

Poté tedy kvalitu řešení IS/ICT specifikuje, jaká je používána platforma pro provoz. Je tedy také nutné volit správné jednotlivé prvky tak, aby spolu vzájemně co nejlépe spolupracovaly.[16]

[15] SODOMKA, Petr. Informační systémy v podnikové praxi. Vyd. 1. Brno: Computer Press, 2006, 351 s. ISBN 80-251-1200-4, str. 74

[16] SODOMKA, Petr. Informační systémy v podnikové praxi. Vyd. 1. Brno: Computer Press, 2006, 351 s. ISBN 80-251-1200-4, str. 74-75

1.2.5 ERP systém

„Informační systém kategorie ERP definujeme jako účinný nástroj, který je schopen pokrýt plánování a řízení hlavních interních podnikový procesů (zdrojů a jejich transformace na výstupy), a to na všech úrovních od operativní až po strategickou.“[17]

Jde tedy o procesy jako je výroba, (interní) logistika, personalistika a ekonomika (např. finance, účetnictví, controlling).

ERP systémy dělíme podle oborového a funkčního zařízení. EPR systém nemusí pokrývat všechny interní procesy. Rozlišují se 3 typy ERP systémů:

- All–in–One: pokrývá všechny interní podnikové procesy, tj. personalistiku, výrobu, logistiku a ekonomiku. Mezi jeho výhody patří vysoká úroveň integrace. Nevýhody jsou zejména nižší detailnost a nákladné přizpůsobení systému podniku.
- Best-of-Breed: je orientován na určité obory podnikání nebo specifické procesy. Nemusí pokrývat všechny klíčové procesy. V rámci podniku může existovat společně s jinými IS. Jeho výhodou je tedy detailní funkcionalita a nevýhodou může být obtížnější sledování a řízení procesů a nutnost řešení více IT projektů.
- Lite ERP: je okleštěná verze standardního ERP systému. Je zaměřena většinou na malé a středně velké podniky, které si zpravidla nemohou dovolit platit za standardní ERP systém. Výhodou je tedy nižší cena a rychlá implementace do podniku. Nevýhodou je omezení množství funkcí nebo počtu uživatelů, popřípadě možnosti rozšíření apod.

Praxe v podnicích postupně začala vyžadovat propojení interních a externích procesů (jedná se o oblast řízení vztahu se zákazníky a řízení dodavatelského řetězce). U těchto procesů není tedy přesně určen vlastník a management v podniku nemá jejich řízení přímo pod kontrolou. Proto se ERP systémy rozšířily do podoby označované jako ERP II, někdy nazývané též rozšířené ERP (Extended ERP).[18]

---

[17] SODOMKA, Petr. Informační systémy v podnikové praxi. Vyd. 1. Brno: Computer Press, 2006, 351 s. ISBN 80-251-1200-4, str. 86

[18] SODOMKA, Petr. Informační systémy v podnikové praxi. Vyd. 1. Brno: Computer Press, 2006, 351 s. ISBN 80-251-1200-4, str. 86-88

V ERP systémech se používají tři základní přístupy k zefektivnění fungování podniku:

- JIT – Just in Time – je charakterizován včasnými dodávkami zboží, založen na tažném principu (materiálové požadavky na díly táhne v podobě objednávek od zákazníka k dodavateli),
- MRP II – Manufacturing Resources Planning – založen na tlačném principu (zaměřuje se na splnění termínu dodávky zboží, na základě uspořádání výrobku stanovuje termíny pro objednání materiálu a zahájení jednotlivých fází výroby),
- TOC – Theory of Constraint – je překládán jako teorie omezení. Zaměřuje se na optimalizaci a úzká místa. Je kombinací tažného a tlačného principu, kde právě pro plánování je tzv. úzké místo důležité.[19]

1.3 EFEKTIVNOST INFORMAČNÍCH SYSTÉMŮ

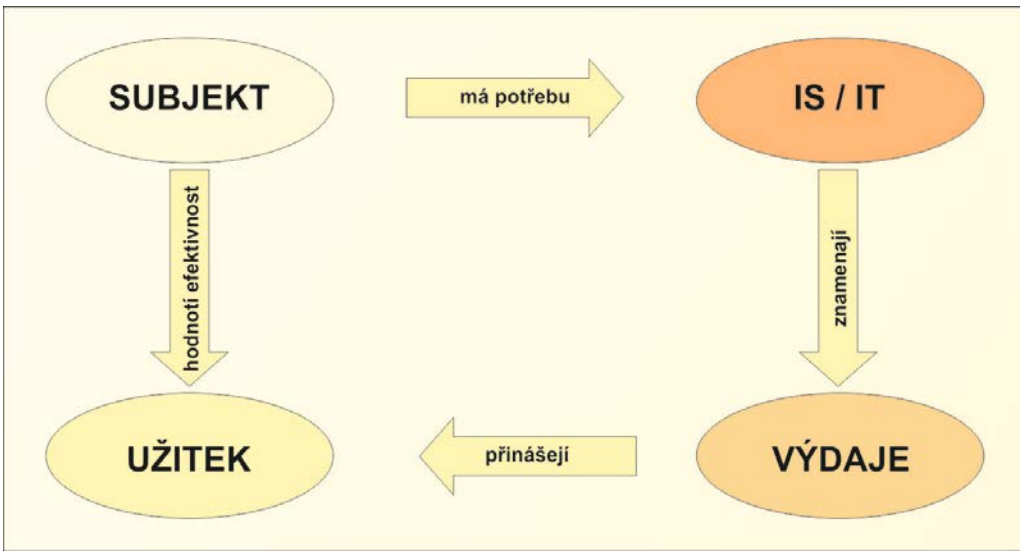
1.3.1 Užitek z IS/IT

Užitek z IS souvisí s efektivností IS - potřebou informací vzniká požadavek na určitý informační systém. Z uspokojení této potřeby je nějaký užitek. Potřebu IS uspokojí určitá aplikace IT, která ovšem přináší náklady (stojí peníze). Pokud je potřeba uspokojení informací vysoká, je i vysoký užitek. Předpokládáme pak, že i efektivnost vynaložených prostředků bude vysoká.

Užitek (utility) je v podstatě uspokojení nějaké potřeby – musí mít pro určitý subjekt určitý význam. [20]

[19] BASL, Josef. Podnikové informační systémy: podnik v informační společnosti. 2., výrazně přeprac. a rozš. vyd. Praha Grada, 2008, 283 s. ISBN 978-80-247-2279-5, str. 139-141

[20] MOLNÁR, Zdeněk a Jiří MAREK. Efektivnost informačních systémů. 1.vyd. Praha: Grada Publishing, 2005, 142 s. Expert (Grada). ISBN 80-716-9410-X. str. 16



Obrázek 6 – model užitku

Hodnocení efektivity IS/IT není jen otázkou požadavků (potřeb) a jejich uspokojení. Ale jde zejména o to, co lidé jakožto příjemci užitku, očekávají.

V podniku tedy najdeme 4 kategorie subjektů a jejich očekávání:

- Majitelé – očekávají trvalé zhodnocení vloženého majetku,
- Manažeři – očekávají možnost efektivního řízení, tzn. dosáhnout daných, výsledků s minimem prostředků vynaložených na správu,
- Zaměstnanci – očekávají lepší pracovní prostředí,
- Zákazník - by měl dostat zboží s vyšší přidanou hodnotou za přijatelnou cenu.

Každý subjekt hledá optimální poměr mezi užitkem IS/IT a výdaji, které musí vynaložit, časem potřebným pro získání užitku a riziky spojenými s tím, že IS/IT nedosáhne očekávaného užitku.

Výdaje do IS jsou pro subjekt (majitele nebo manažery) „viditelné“, kdežto přínosy už tak viditelné nejsou. V hospodaření podniku se přínosy z IS/IT projevují nepřímo, kde nelze poté určit, jestli rozhodnutí řídícího pracovníka bylo dáno jeho intuicí nebo bylo založeno na informacích získaných z informačního systému. Další věc je ta, že je IS pořizován na delší dobu a jeho výsledky se také projevují až po delší době, a za tuto dubu se už pozapomnělo, jaké vůbec bylo očekávání, požadavky a cíle informačního systému na počátku jeho zavádění. [21]

[21] MOLNÁR, Zdeněk a Jiří MAREK. Efektivnost informačních systémů. 1.vyd. Praha: Grada Publishing, 2005, 142 s. Expert (Grada). ISBN 80-716-9410-X. str. 16,17

„Celá řada výzkumů Mahmoos and Mann (1993), Shaw (1994), Berndt and Morrison (1995), Brynjolfsson and Young (1996) ukázala, že investice do IS/IT nepřinášejí očekávané efekty ve smyslu ekonomické návratnosti, (např., že jeden investovaný USD do IS/IT přinese jen 0,8 USD). Tato zjištění vedla zmíněné autory k tomu, co nazývají paradoxem informační technologie nebo také paradoxem efektivity. Byla nastolena otázka: „Proč produktivita práce neroste současně s používáním pokrokových IT?“. Brynjolfsoon má pro tento paradox následující vysvětlení:

1) *Používání nesprávných resp. nevhodných závislostí výstupů na vstupech*
2) *Velkým časovým odstupem mezi vstupem (investicí) do IS/IT a výstupem (přínosem)*
3) *Působením faktoru redistribuce přínosů, který se uplatňuje tak, že konkurenční výhoda, kterou získá některý podnik v důsledku pionýrské aplikace IS/IT je rychle absorbována ostatními podniky*
4) *Špatným řízením investic do IS/IT způsobujícím zbytečné investice resp. které jsou ztrátové.“*[22]

1.3.2 Model efektivnosti IS/IT

Obrázek 7 – koncepční schéma modelu efektivnosti

Zkoumání efektivnosti IS/IT může být založeno na obecném modelu přeměny vstupů na výstupy, pokud působí činitelé (vnější i vnitřní), které ovlivňují efektivnost této změny.[23]

[22] MOLNÁR, Zdeněk a Jiří MAREK. Efektivnost informačních systémů. 1.vyd. Praha: Grada Publishing, 2005, 142 s. Expert (Grada). ISBN 80-716-9410-X. str. 17

[23] MOLNÁR, Zdeněk a Jiří MAREK. Efektivnost informačních systémů. 1.vyd. Praha: Grada Publishing, 2005, 142 s. Expert (Grada). ISBN 80-716-9410-X. str. 18

Na tomto modelu se hledají odpovědi na otázky: Jak řídit rozvoj IS/IT tak, abychom (i přes velmi omezené výdaje) dosáhli co největšího přínosu pro podnik? V dalším případě, který je lepší, se už hledá odpověď na otázku: Jaké mají být vstupy pro dosažení požadovaných přínosů? V tomto modelu se pak pro dosažení efektivnosti minimalizují vstupy a maximalizují výstupy. Nejdůležitější je najít činitele, kteří tuto změnu ovlivňují nejvíce.[24]

1.3.3 Informační strategie

Informační strategií se rozumí soustava cílů a způsobů jak těchto cílů dosáhnout. Cílem je tedy odpovědět na následující otázky, jak dosáhnout pomocí IS/IT:

- zvyšování výkonnosti pracovníků,
- podporování strategických cílů podniku,
- získávání konkurenčních výhod pro podnik,
- vytváření strategických příležitostí rozvoje pro podnik.

Definování této strategie je výsledkem trvalého dialogu mezi oddělením IS/IT nebo odborníky informatiky, kteří můžou být interní nebo externí, a managementem podniku. Tento dialog by měl být zaměřen zejména na analýzu procesů (vnitřních i vnějších) a jak tyto procesy lze podpořit pomocí IS/IT, pokud možno včetně vytváření informační infrastruktury.

Informační infrastruktura je v podstatě zázemí (prostředí) pro rozvoj IS/IT. Je vhodné, aby informační infrastruktura tj. její úroveň, mírně a trvale předbíhala celkovou úrovně IS/IT. Neměla by se poté stát brzdou pro rozvoj IS/IT.

Celková úroveň je dána úrovní jednotlivých jejich složek, proto je nutné, aby její jednotlivé složky byly na odpovídající a vyrovnané úrovni[24].

Komponenty infrastruktury[24]:

- hardware – dostatečně výkonné vybavení, včetně síťových prvků,
- základní software – vhodné operační systémy a databázový software,
- dataware – správné datové zdroje,
- peopleware – dostatečné informační a počítačové povědomí zaměstnanců,

[24] MOLNÁR, Zdeněk a Jiří MAREK. Efektivnost informačních systémů. 1.vyd. Praha: Grada Publishing, 2005, 142 s. Expert (Grada). ISBN 80-716-9410-X. str. 18,19

- orgware – organizační struktura podniku slučitelná s informačním systémem a systémem řízení podniku.

1.4 METODA HOS

Jedná se o metodu vyvinutou Ústavem informatiky Fakulty podnikatelské VUT v Brně. V této metodě je ucelený pohled na informační systém realizován na základě 8 oblastí:

- Hardware – zkratka HW
- Software – zkratka SW
- Orgware – OW
- Peopleware – PW
- Dataware – DW
- Customers – CU
- Suppliers – SU
- Management IS – MA[25]

1.4.1 Oblasti hodnocení

Hardware – zkoumá se fyzické vybavení v závislosti na jeho spolehlivosti, bezpečnosti a funkčnosti společně se softwarem.

Software – zabývá se zkoumáním programového vybavení, zaměřuje se zejména na funkce tohoto vybavení a jak obtížné je jeho používání a ovládání.

Orgware – tato oblast obsahuje pravidla pro provoz IS a doporučené pracovní postupy

Peopleware – v této oblasti jsou zkoumáni uživatelé IS a jaký je jejich postoj k rozvoji vlastních schopností, dále podpora při užívání IS a jak vnímají jeho důležitost.

Metoda HOS 8 nemá za úkol jakkoliv hodnotit odborné kvality uživatelů a míru jejich schopností.[25]

Dataware – v této oblasti je zkoumáno, kde jsou v IS data uložena a používána v souvislosti na jejich dostupnosti, správě a bezpečnosti. Tato metoda nehodnotí množství dat

[25] KOCH, Miloš a Kol. Management informačních systémů. Vyd. 2., přeprac. Brno: Akademické nakladatelství CERM, 2010, 171 s. Učební texty vysokých škol. ISBN 978-80-214-4157-6, str. 67-68

uložených v IS, nebo jaká je jejich přesnost. Je zaměřena na způsob jejich využití uživateli a způsobem jejich správy.

Customers (zákazníci) – v této oblasti je předmětem zkoumání co má IS svým zákazníkům poskytovat a způsob řízení této oblasti. Pojem zákazníci je závislý na zkoumaném IS, může se jednat jak o zákazníky v obchodním pojetí, tak i vnitropodnikové, kteří používají výstupy ze zkoumaného IS. V této oblasti není zkoumána spokojenost zákazníků se stavem IS, ale jaký je způsob řízení u této oblasti v podniku.

Suppliers (dodavatelé) – tato oblast zkoumá způsob řízení této oblasti a co vyžaduje od svých dodavatelů IS. Podobně jako u CU dodavatelé IS mohou být jak obchodní, tak i vnitropodnikoví, kteří dodávají IS služby, výrobky či informace, které mají souvislost s těmito výkony. V této oblasti není předmětem zkoumání spokojenost podniku s existujícími dodavateli.

Management IS – v této oblasti se zkoumá, jaká je závislost informační strategie a řízení informačních systémů, důslednost používání daných pravidel a jak vnímají koncoví uživatelé informační systém. Tato metoda nehodnotí znalosti managementu IS.[26]

1.4.2 Kritéria pro oblasti metody a způsob odpovědí na otázky

K výše popsaným oblastem autoři metody nalezli kritéria, která přeformulovali do kontrolních otázek, jež pomohou identifikovat, jaký je stav v dané oblasti zkoumaného IS.

Tato metoda není schopna postihnout všechny vazby a prvky v posuzovaných oblastech. Byly nalezeny jen prvky a vazby v IS, které mají největší vliv na celkový stav zkoumané oblasti.

U každé kontrolní otázky se odpovídá výběrem jedné z pěti možných odpovědí. Pro většinu otázek je používáno následující slovní vyjádření:

Ano | spíše ano | částečně | spíše ne | ne

Toto slovní hodnocení je poté transformováno do celočíselné stupnice od 5 do 1, kde:

5 = ANO až 1 = NE

V případě, kdy u otázky odpověď NE vypovídá o vysokém stavu v dané oblasti, je transformována opačným způsobem. Tj.: 1 = ANO až 5 = NE[26]

[26] KOCH, Miloš a Kol. Management informačních systémů. Vyd. 2., přeprac. Brno: Akademické nakladatelství CERM, 2010, 171 s. Učební texty vysokých škol. ISBN 978-80-214-4157-6, str. 68-69

V této metodě je převod hodnot odpovědí na čísla prováděn až po zodpovězení otázek pro všechny oblasti.

Výpočet pro stav oblastí je prováděn pomocí následujícího vzorce. Tento vzorec je platný pro všech osm oblastí:

$$u_i = \left[\frac{\sum_{j=1}^{10} u_{ij} - MAX_i - MIN_i}{8} + 0{,}5 \right]$$

Kde:

i je i- tá oblast

j je pořadové číslo otázky

u_i je hodnota stavu oblasti

u_{ij} je bodové vyjádření oblasti na j- tou otázku v i- té oblasti

MAX_i je maximální hodnota zjištěné odpovědi z otázek v dané oblasti

MIN_i je minimální hodnota zjištěné odpovědi z otázek v dané oblasti

Stav zkoumané oblasti, stejně jako souhrnný stav IS, je vyjádřen hodnotou v rozmezí od 1 do 5. Celkový stav IS *u* je v této metodě určen nejnižší hodnotou ze všech hodnocení oblastí.

$u(_i) = 5$: velmi vysoká úroveň oblasti *i* / stavu informačního systému

$u(_i) = 4$: vysoká úroveň oblasti *i* / stavu informačního systému

$u(_i) = 3$: střední úroveň oblasti *i* / stavu informačního systému

$u(_i) = 2$: nízká úroveň oblasti *i* / stavu informačního systému

$u(_i) = 1$: velmi nízká úroveň oblasti *i* / stavu informačního systému

Za vyvážený informační systém se považuje ten, ve kterém se vyskytují pouze dvě sousední hodnoty, přičemž jedna hodnota *u* zde musí převažovat. Rozlišuje se i zcela vyvážený systém, ve kterém jsou všechny hodnoty *u* stejné. Za nevyvážený informační systém se považuje ten, ve kterém v hodnocení oblastí jsou alespoň 3 různé hodnoty, popřípadě je rozdíl v hodnocení oblastí větší nebo roven 2 oproti souhrnnému stavu *u*.

V metodě HOS jsou rozlišovány tři stavy důležitosti informačního systému - v, kde *v* nabývá hodnot -1, 0, 1.

v = -1 – informační systém není pro chod firmy důležitý

v = 0 – informační systém je pro firmu důležitý, ovšem jeho krátkodobý výpadek nebude mít vliv na chod firmy

v = 1 – informační systém je pro firmu důležitý, jeho krátkodobý výpadek může výrazně ovlivnit fungování firmy.[27]

Omezení metody HOS 8:

- *„Tato metoda není určena k detailnímu zkoumání IS na úrovni jednotlivých procesů*
- *Výsledky metody jsou založeny na subjektivních odpovědích na kontrolní otázky*
- *Kontrolní otázky jsou všeobecné kvůli relativně širokému záběru zkoumaných informačních systémů“*[28]

1.5 RIZIKO

Riziko má mnoho definic, které také záleží na odvětví, oboru a problematice. Záleží též na jazyku, např. v češtině má riziko záporný charakter.

1) *„pravděpodobná hodnota ztráty vzniklé nositeli popř. příjemci rizika realizace scénáře nebezpečí vyjádřená v peněžních nebo jiných jednotkách“*
2) *„kumulativní účinek pravděpodobnosti nejisté události, která může pozitivně nebo negativně ovlivnit cíle projektu“*
3) *„kombinace pravděpodobnosti a škody“*[29]

[27] KOCH, Miloš a Kol. Management informačních systémů. Vyd. 2., přeprac. Brno: Akademické nakladatelství CERM, 2010, 171 s. Učební texty vysokých škol. ISBN 978-80-214-4157-6, str. 72-76

[28] KOCH, Miloš a Kol. Management informačních systémů. Vyd. 2., přeprac. Brno: Akademické nakladatelství CERM, 2010, 171 s. Učební texty vysokých škol. ISBN 978-80-214-4157-6, str. 83

[29] BASL, Josef. Podnikové informační systémy: podnik v informační společnosti. 2., výrazně přeprac. a rozš. vyd. Praha: Grada, 2008, 283 s. ISBN 978-80-247-2279-5, str. 16

1.6 INFORMAČNÍ BEZPEČNOST

Informace jsou aktivum, které je nevyhnutelné pro činnost organizace, a je tedy potřebné, aby byly přiměřeně chráněny.

Jak již bylo výše zmíněno, informace existují v mnoha různých podobách, ať již tištěné nebo napsané na papíře, též uložené elektronicky, přenášené poštou, nebo použitím elektronických prostředků. Informace mohou být také vyslovené v konverzacích.

Informační bezpečnost je ochrana informací před širokou škálou hrozeb, jejímž cílem je:

- Zabezpečení spojitosti činností bez zbytečných přerušení
- Minimalizovat podnikatelské riziko
- Maximalizovat využití investic a obchodních příležitostí

Hrozba – možná příčina nežádoucího incidentu, který může vyústit do poškození systémů nebo organizace

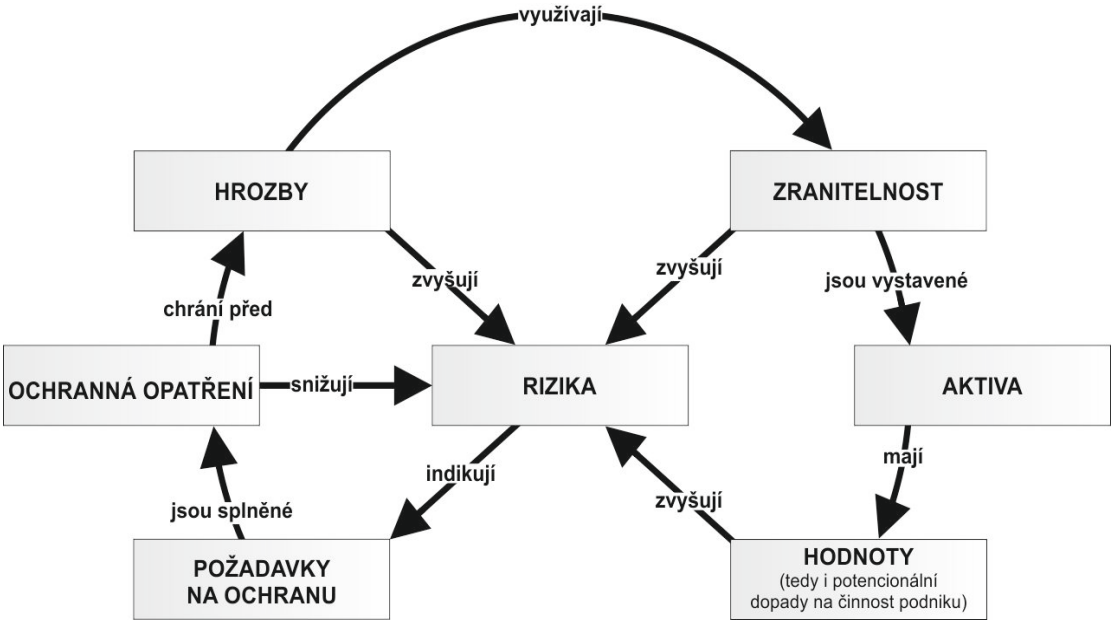
Incident informační bezpečnosti – jedna nebo více nežádoucí a neočekávané události informační bezpečnosti, při kterých je vysoká pravděpodobnost kompromitace aktivit organizace a ohrožení informační bezpečnosti.

Informační bezpečnost – je zachování důvěrnosti, integrity a dostupnosti informací. Může se týkat i dalších vlastností, jakými jsou autentičnost, sledovatelnost, nemožnost popřít zodpovědnost a spolehlivost.

Následující prvky mají vliv na informační bezpečnost, jejich vztahy jsou znázorněny na obrázku:

- Aktiva,
- Dopady,
- Hrozby,
- Zranitelnost,
- Rizika,
- Požadavky na ochranu,
- Ochranné opatření.[30]

[30] STRNÁD, Ondrej. Systémový prístup k riadeniu informačnej bezpečnosti. 1. vyd. Trnava (Slovensko): SP Synergia, 2008. 233 s. ISBN 978-80-89291-20-5, str. 17, 18, 21, 25



Obrázek 8 – vztahy mezi informačními prvky

Z obrázku vyplývá:

Hrozby využívají existujících zranitelností aktiv pro ohrožení hodnot, které aktiva pro podnik představují. Hrozby tedy zvyšují rizika vzniku bezpečnostních incidentů.

Zranitelnosti využívají hrozby pro ohrožení aktiv a zvyšují riziko vzniku bezpečnostních incidentů.

Rizika představují požadavky pro provedení bezpečnostních opatření. Čím je riziko vyšší, tím důkladněji poté musí být provedena ochranná opatření.

Ochranná nebo-li bezpečnostní opatření, chrání aktiva před hrozbami, které mohou využít existujících zranitelností pro ohrožení aktiv. Potom tedy bezpečnostní opatření snižují rizika vzniku bezpečnostních incidentů.

Aktiva organizace obsahují: počítačový hardware, komunikační prostředky, informace, data (dokumenty, databáze, soubory), software, schopnost tvorby produktů popř. poskytování služeb, zaměstnance a nehmotné hodnoty jako je např. dobré jméno společnosti.[31]

Hrozby mohou být přírodního (požár, povodeň,…) nebo lidského původu. Ty, které mají lidský původ, mohou být úmyslné (odposlouchávání, krádež,…) a náhodné (chyby a

[31] STRNÁD, Ondrej. Systémový prístup k riadeniu informačnej bezpečnosti. 1. vyd. Trnava (Slovensko): SP Synergia, 2008. 233 s. ISBN 978-80-89291-20-5, str. 25-27

opomenutí, vymazání souboru,…) Mezi největší hrozby patří vlastní a bývalí zaměstnanci, včetně správců systému, počítačové viry, informační špionáž, …

Dopad je důsledek nežádoucího incidentu a má vliv na aktiva organizace, jako je např. zničení určitých aktiv, ztráta funkčnosti, důvěrnosti, dostupnosti, … Dopad bezpečnostních incidentů má také finanční ztráty a může mít vliv na ztrátu podílů na trhu nebo ztrátu dobrého jména organizace.

Riziko zde vyjadřuje možnost, že hrozba využije zranitelnosti systému nebo organizace, proto, aby způsobila ztrátu nebo poškození aktiv, popř. skupiny aktiv. Tedy přímo či nepřímo poškodila podnik. Rizikový scénář poté popisuje, jak může konkrétní hrozba nebo skupina hrozeb zranitelnost využít. Riziko charakterizuje kombinace dvou faktorů, tj. pravděpodobnost výskytu nežádoucího jevu (incidentu) a jeho dopadu.

Zůstatkové riziko – rizika i přes použití ochranných opatření nelze zcela odstranit. Také platí, že pro zmírnění následků bezpečnostního incidentu, je třeba vynaložit finanční prostředky. Proto čím mají být nižší následky bezpečnostních incidentů, tím vyšší se musí vynaložit náklady.

Bezpečnostní opatření – jsou většinou nazývána jako ochranná a jsou to praktiky, postupy nebo mechanizmy, které nám mohou poskytnout ochranu před hrozbou nebo omezit dopad nežádoucího incidentu, zjistit nežádoucí incidenty a ulehčit obnovu. Ochranná opatření tedy mohou mít jednu nebo více funkcí (např. zjišťování, prevence, omezení, monitorování,…)

Příklady bezpečnostních opatření – antivirový software, záložní kopie, rezervní zdroje energie, šifrování dat,….

Omezení – při řešení bezpečnosti jsou obvykle dané vedením organizace, část plyne z prostředí, ve kterém organizace provádí svoji činnost. Mohou být organizační, finanční, personální, právní nebo kulturně-sociální,…[32]

[32] STRNÁD, Ondrej. Systémový prístup k riadeniu informačnej bezpečnosti. 1. vyd. Trnava (Slovensko): SP Synergia, 2008. 233 s. ISBN 978-80-89291-20-5, str. 28-36

2 Praktická část

2.1 O organizaci

Název organizace: Mateřská škola Boskovice, okres Blansko

Sídlo organizace: Lidická 1690, 1691; 680 01 Boskovice

Forma organizace: příspěvková organizace

Identifikační číslo: 620 728 71

Zřizovatel: Město Boskovice, Masarykovo náměstí 4/2, 680 18 Boskovice IČ 00279978, okres Blansko.

Hlavní účel a předmět činnosti: Organizace byla zřízena pro zajištění činnosti zřizovatele v oblasti školství, dle zákona č 561/2004 Sb., o předškolním, základním, středním, vyšším odborném a jiném vzdělávání (školský zákon), ve znění pozdějších předpisů. Předmětem činnosti je tedy odpovídající vymezení hlavního účelu příspěvkové organizace, tedy výkon činnosti mateřské školy a zařízení školního stravování.

Zřizovatel povolil následující okruhy doplňkové činnosti

- Výrobu a prodej výrobků a výpěstků,
- Obchodní a obdobnou činnost,
- Poskytování prací a služeb,
- Pronájem kapacit sloužících k plnění úkolů v hlavní činnosti v době, ve které nejsou pro tento účel využity

Aktuální podoba organizace byla zřízena k 1. 7. 2008, kdy právně došlo ke zrušení dvou mateřských škol, a nástupnickou organizací se stala, MŠ Lidická, následně byl změněn název, jak je uveden výše. Tedy původní příspěvkové organizace zřízené na konci roku 1994 se sloučily do jednoho komplexu, složeného ze tří samostatných budov, kde je celkem 18 tříd, s celkovou povolenou kapacitou pro 415 dětí.

Stávající organizace čítá přibližně 70 zaměstnanců a organizace pro svoji činnost využívá tří budov sídlících na ulicích Lidická, která slouží jako sídlo, Na Dolech a Bílkova ul[33].

[33] http://www.msboskovice.cz/o-nas-2; Zřizovací Listiny příspěvkové organizace; Dodatek č. 7 ke zřizovací listině

2.1.1 Organizační struktura

V čele příspěvkové organizace stojí ředitelka, která je jmenována a odvolávána Radou města Boskovice. Ředitelce jsou podřízeny zástupkyně z každého pracoviště a stravovací provoz každého pracoviště. Zástupkyním pro jednotlivá, pracoviště poté podléhají pedagogičtí a ostatní správní zaměstnanci (většinou uklízečky, školníci). Zaměstnanci kuchyně podléhají vedoucí stravování stravovacího provozu.

Ředitelce dále podléhá správce budov a účetní a personalista.

2.2 Vývoj IS v organizaci a stávající IS

Od vzniku příspěvkové organizace byla agenda účetnictví zpracovávána ručně, mzdy zajišťoval Školský úřad a později Služba škole Blansko.

Od roku 1996 bylo zpracováváno účetnictví v účetním programu Vema pod operačním systémem MS-DOS. Evidence majetku byla vedena pomocí tabulkového procesoru v programu Klasik asistent. Stravovací provoz (evidence strávníků, plateb, příjmů a výdejů potravin) byla zpracovávána ručně až do roku 2003.

V roce 2003 byl zakoupen nový počítač již s OS Windows XP, pro zpracovávání účetnictví. Evidence majetku byla stále vedena pomocí tabulkového procesoru, tentokrát již součástí kancelářského balíku MS Office XP. Od roku 2004 se začaly zpracovávat mzdy v programovém vybavení Vema.

V tomto roce bylo zakoupeno programové vybavení pro stravovací provoz od firmy Barda SW,HW - SW Jídelna, verze 6.3x (MS-DOS). Tento produkt byl, používán do sloučení MŠ, tj do roku 2008. Po sloučení MŠ samozřejmě došlo k nárůstu administrativy.

Po sloučení koncem roku 2008 se zakoupil pro jídelny nový software (pro všechny provozy stejný) od f. Luňák Jídelna, již pracující na systému Windows. Byl též přikoupen modul od Vemy zpracovávající majetek, pokladna a mzdy od různých zpracovatelů naštěstí vše pod Vemou se sloučily do jednoho a organizace si je začala zpracovávat na vlastním programovém vybavení - též od společnosti Vema. V roce 2011 byl přikoupen modul Vemy pro bankovní aplikace, tj. pro zpracování příkazů z mezd do banky, do této doby, byly odnášeny v papírové podobě do banky.

2.2.1 Aktuální stav

Jak již vyplývá z historického vývoje je aktuálně využíván Jídelna a Vema a pro kancelářské aplikace jsou používány kancelářské balíky MS Office.

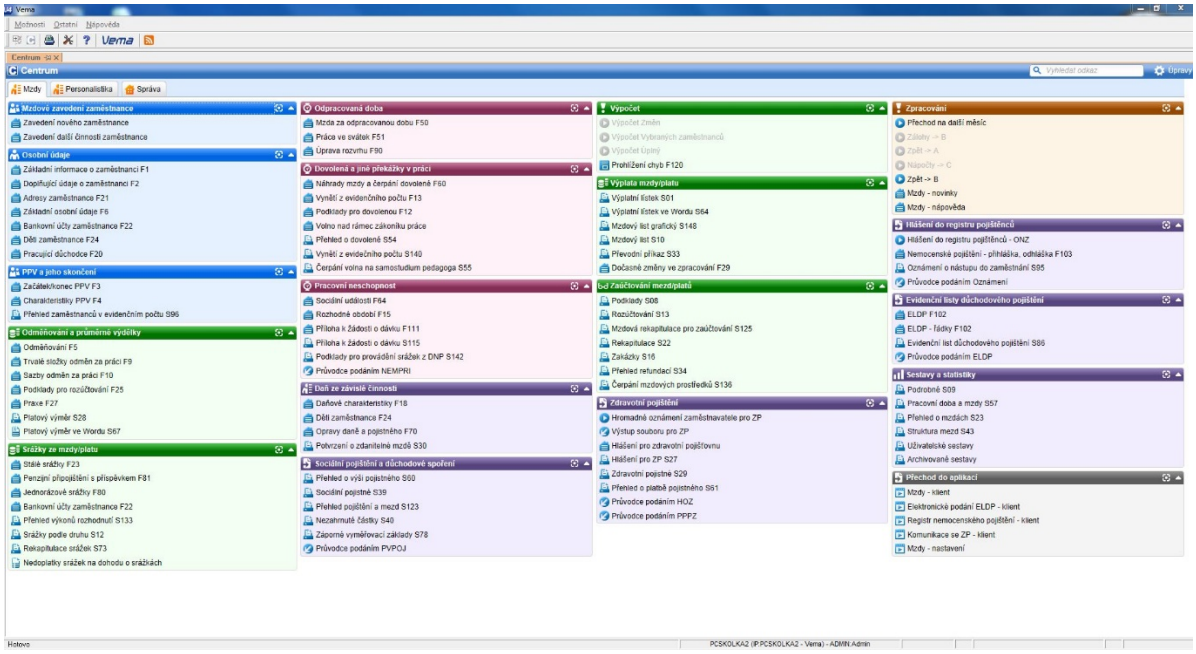
VEMA

V současné době je využíváno řešení od společnosti Vema, v aktuální verzi Vema V4 server s následujícími součástmi:

- V4 Server
  - *Obsahuje všechny potřebné součásti pro běh systému jak na straně klienta, tak i serveru, ale i pro instalaci na jednom počítači*[34].
- Elektronické podání ELDP (Evidenční list důchodového pojištění),
  - *Aplikace, která sdílí data mezi aplikací Mzdy a a technicky zajišťuje komunikaci s Portálem veřejné správy*[34].
- Převodní příkazy KB-formát KM (ABO),
  - *Jedná se konverzní modul k aplikaci Mzdy a slouží k vytváření převodních příkazu do banky ve formátu, a tvaru, který banka akceptuje*[34].
- Komunikace se ZP (zdravotními pojišťovnami),
  - *Umožnuje přímou komunikaci systému Vema s informačními systémy zdravotních pojišťoven, zejména pro podání Hromadného oznámení zaměstnavatele a přehledu o platbě pojistného. Tato komunikace nevyžaduje přímý zásah uživatele a jeho znovu přihlašování*[34].
- Mzdy,
  - *Jedná se o jeden z nejrozšířenějších systému pro zpracování mezd. Výpočet probíhá podle logické návaznosti od vstupních údajů po výstupní údaje pro pojišťovny, bankovní ústavy a orgány sociálního zabezpečení.*
  - *Je v souladu s platnou legislativou,*
  - *Umožnuje automatické roční zúčtování daně,*
  - *Výpočty průměrných a pravděpodobných výdělků, automatické platové postupy, podle předpisů*[34]

[34] http://www.vema.cz/default.aspx?categoryID=Produkty.1

Na následujícím obrázku je znázorněno výchozí uživatelské rozhraní pro mzdy



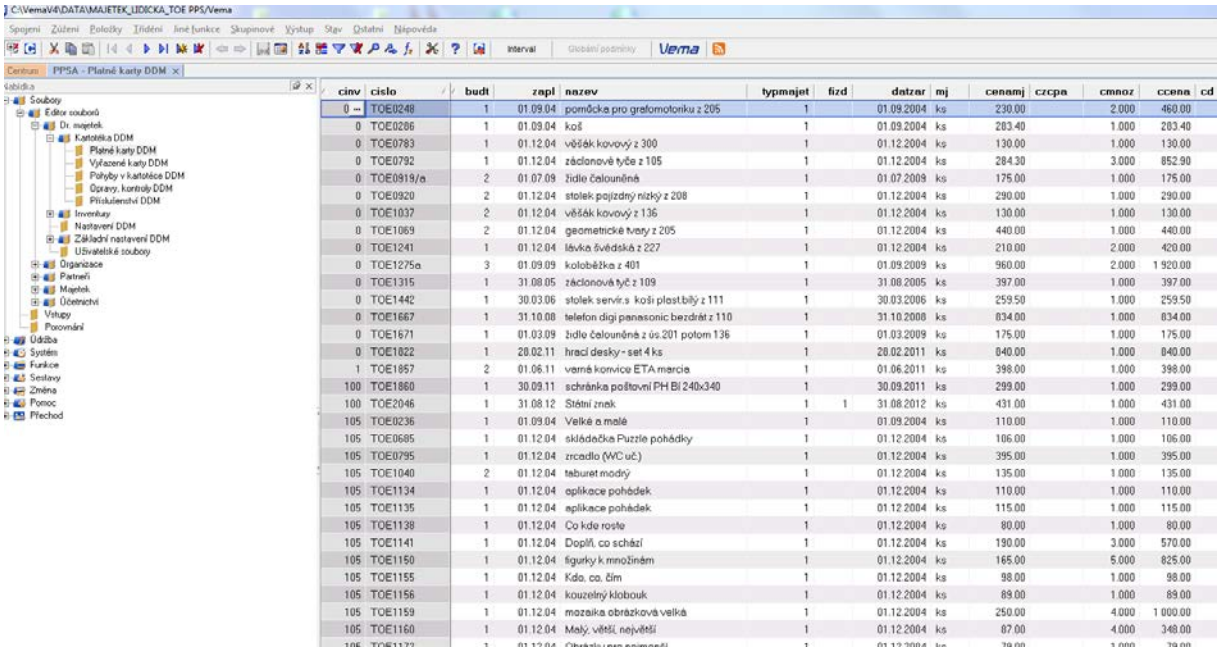
Obrázek 9 – vstupní rozhraní Mzdy systému Vema

- Personalistika,
  - *Slouží k vedení údajů o zaměstnancích,*
  - *Umožnuje osobní údaje zaměstnanců, kontakty, vzdělání,*
  - *Předchozí zaměstnání,*
  - *pracovní a životní jubilea*[35].
- Pokladna,
  - *Součást IS EKOS, zpracovává hotovostní toky a umožnuje přehled o stavu peněžních prostředků,*
  - *Umožnuje zpracování tuzemských i zahraničních cest*[35].
- Registrace nemocenského pojištění,
  - *slouží k podání přihlášek a odhlášek zaměstnanců k nemocenskému pojištění elektronickou formou. Jedná se o doplňkovou aplikaci, která sdílí data s aplikací Mzdy a technicky zajišťuje komunikaci s Portálem veřejné správy*
  - *Na rozdíl od důchodového pojištění jsou zde data zpracovávána po dnech, z důvodu platné legislativy, zejména kvůli termínu pro hlášení změn*[35].

[35] http://www.vema.cz/default.aspx?categoryID=Produkty.1

- Účetnictví,
  - *Je součástí IS EKOS, kde poskytuje vedení účetních knih, kompletní zpracování daňové evidence a výkazů,*
  - *Obsahuje legislativní servis (vždy aktuální legislativa pro výkazy atd.),*
  - *Podporuje vícezdrojové financování a vykazování grantů.* [36]
- Dlouhodobý majetek.
  - *Eviduje majetek, kde údaje o tomto majetku jsou ve formě karet, kde jsou údaje o tomto majetku*
  - *Tisk je umožněn i s tříděním podle zadaných hledisek.*[36]
- Drobný majetek,
  - *K vedení evidence o drobném majetku,*
  - *Umožnuje tisknout jak hromadné sestavy, tak i jeho členění podle různých hledisek*[36].

Na následujícím obrázku je přehled karet drobného dlouhodobého majetku, kde Vema v tomto řádkovém provedení pro názvy sloupců v celém systému používá zkratek, kde význam zkratky se zobrazí po najetí kurzoru na zkratku nebo je možné použít formulářový tvar jedné položky, kde je použit celý název.



Obrázek 10 – Přehled karet DDM IS Vema

[36] http://www.vema.cz/default.aspx?categoryID=Produkty.1

Systém Evidence jídelny 2014

Evidence jídelny od L.V.-software

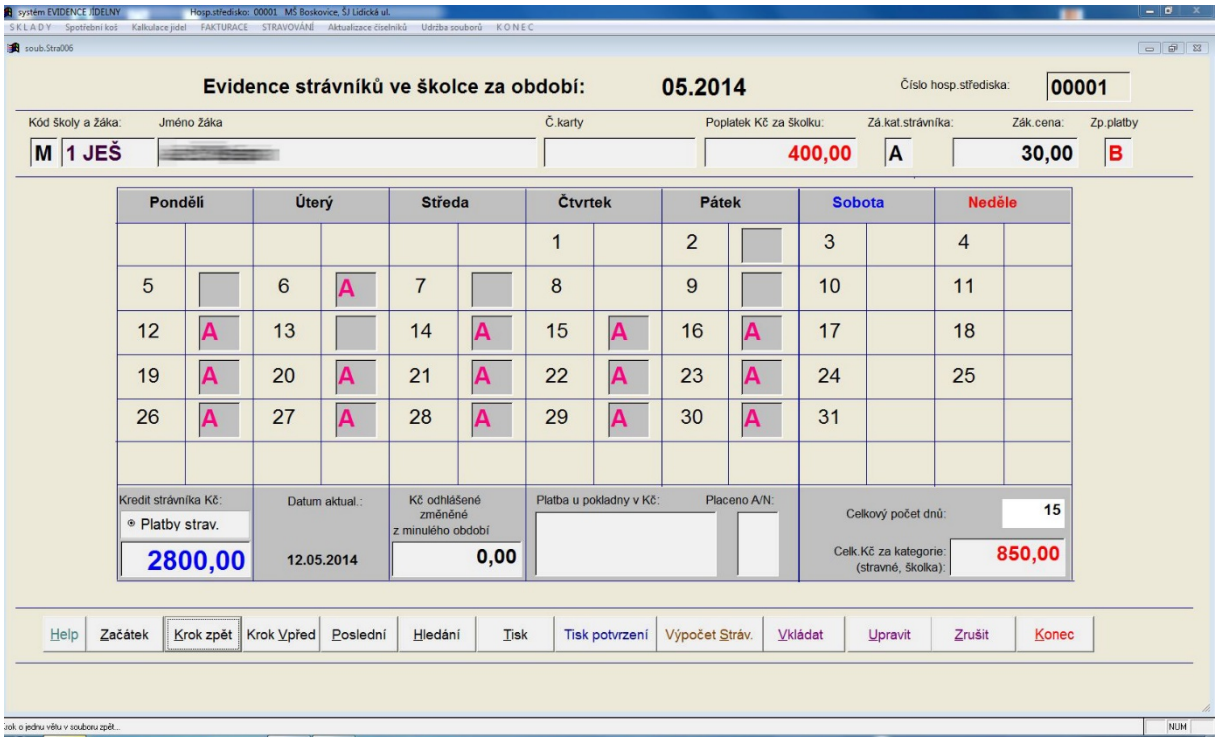
Obsahuje moduly pro kompletní zpracování agendy stravovacích provozů, podle platné legislativy, také umožňuje zřízení více hospodářských středisek v jednom programu.

- Dodací listy- příjemky, knihu výdejů – výdejky (potravin), Kniha faktur
- Výpočet spotřebního koše – sleduje procentuální plenění spotřeby jednotlivých komodit potravin, jejichž množství pro měsíc je udáno legislativou.
- Inventarizaci skladu (zásob, které by měly být na skladě),
- Evidence strávníků, která umožnuje tisknutí sestav měsíčních nebo denních odběrů stravy po třídách nebo kompletní, včetně formuláře pro měsíční odběry stravy, evidence obsahuje kategorie strávníků podle
- Evidence plateb a přeplatků či nedoplatků strávníků (Platby strávníků),
- Pokladna a přehled hospodaření jídelny (poměr mezi výdejem potravin ze skladu, k ceně potravin, kterou zaplatí strávníci.

Systém umožňuje přímé sehrání došlých plateb od strávníků ze souboru, který poskytuje banka – přiřazuje je podle variabilního symbolu strávníka. Podobným způsobem umožnuje export přeplatků stravného do banky.[37]

Na následujícím obrázku je ukázka prostředí s evidencí odebrané stravy strávníka. V celém systému se musí dbát na uzavírání otevřených oken tlačítkem Konec vpravo dole, jinak při uzavírání vyskakuje chybové hlášení. Systém Jídelny nelze zavřít křížkem systému Windows a při ukončování systému Evidence jídelny se musí používat v horní liště položka KONEC, která ovšem vybízí i méně zkušené uživatele k archivaci.

[37] Manuál Evidence školní jídelny



Obrázek 11– Systém evidence jídelny – přehled strávníka

Na následujícím obrázku je sestava spotřebního koše, protože přehled plnění jednotlivých komodit v procentech je znázorněn pouze tiskovou sestavou.

Spotřební koš potravin dle vyhlášky 107/2005 Sb., částka 34, str.1114

List: 1
Sestava: JID210K
Datum: 09.05.2014

za období: 04.2014

		Přé.poč.strávníků: 2195	Počty strávníků za jednotlivé kategorie											
			Př.poč.: 2053		Př.poč.: 0		Počet.: 142		Počet.: 0		Počet.: 0			
	Skupina potravin		MŠ 3 - 6 let		MŠ 7 - 10 let		ZŠ 7 - 10 let		ZŠ 11 - 14 let		ZŠ(SŠ) 15 a víc		Nor.celkem	Spotřeba	* %
			No.(g)	Prop.(Kg)	No.(g)	Prop.(Kg)	No.(g)	Prop.(Kg)	No.(g)	Prop.(Kg)	No.(g)	Prop.(Kg)	(Kg)	(Kg)	plnění
A	Maso		55	112,943	0	0,000	89	12,652	70	0,000	70	0,000	125,595	129,270	102,93
B	Ryby		10	20,535	0	0,000	18	2,559	10	0,000	10	0,000	23,094	21,940	95,00
C	Mléko tekuté		300	616,050	0	0,000	150	21,324	70	0,000	100	0,000	637,374	429,785	67,43
D	Mléčné výrobky		31	63,659	0	0,000	42	5,971	17	0,000	9	0,000	69,630	82,454	118,42
E	Tuky volné		17	34,910	0	0,000	21	2,985	15	0,000	17	0,000	37,895	16,502	43,55
F	Cukr volný		20	41,070	0	0,000	33	4,691	16	0,000	16	0,000	45,761	33,433	73,06
G	Zelenina		110	225,885	0	0,000	129	18,339	90	0,000	100	0,000	244,224	177,642	72,74
H	Ovoce		110	225,885	0	0,000	102	14,500	80	0,000	90	0,000	240,385	202,720	84,33
I	Brambory		90	184,815	0	0,000	180	25,589	160	0,000	160	0,000	210,404	109,160	51,88
J	Luštěniny		10	20,535	0	0,000	10	1,422	10	0,000	10	0,000	21,957	12,726	57,96

Obrázek 12 – Systém evidence jídelny – plnění spotřebního koše

2.2.2 Hardware, software a síť

Na všech počítačích je používán operační systém Microsoft Windows XP nebo Windows 7 většinou ve verzi Professional.

Většina zaměstnanců, kteří pracují s počítačem, používá pro svoji práci balík Microsoft Office ve verzích od 2003, 2007 a 2010 většinou ve verzi Standard, který obsahuje nejčastěji používané nástroje. To znamená Outlook pro práci s emaily, protože, většina výměn dokumentů probíhá pomocí e-mailu nebo osobně. Dále je hlavně používán Word, pro přípravu dokumentů jako jsou směrnice, pravidelné zprávy a hlášení od zástupkyň (např. čerpání dovolené, studijního volna, pracovní neschopností a zástupů za nemoc) jako podklady pro mzdy. Vedoucí stravování sice mohou napsat jídelníček v programu Jídelny, ale používají vlastní vytvořené šablony pro jídelníčky. Evidují si též neplatiče z řad strávníků. Excel je využíván pro tabulkové přehledy a zejména seznamy. Kompatibilita mezi formáty je na počítačích kde je přítomen MS Office 2003 zajištěna sadou Microsoft Office Compatibility Pack pro formáty souborů aplikace Word, Excel a PowerPoint, který umožní otevřít dokumenty vytvořené v novějších verzích. Pro vzdálenou pomoc se systémem Evidence školní jídelny je na těchto počítačích přítomen TeamViewer. Společnost Vema pro vzdálenou pomoc využívá svoje programy.

Dále je na jednom počítači nainstalován Pinnacle Studio 15 HD Ultimate Collection CZ a Zoner Photo Studio 14 Pro EDU, které slouží ke zpracování videa a úpravu fotografií (slouží pro reprezentaci školy).

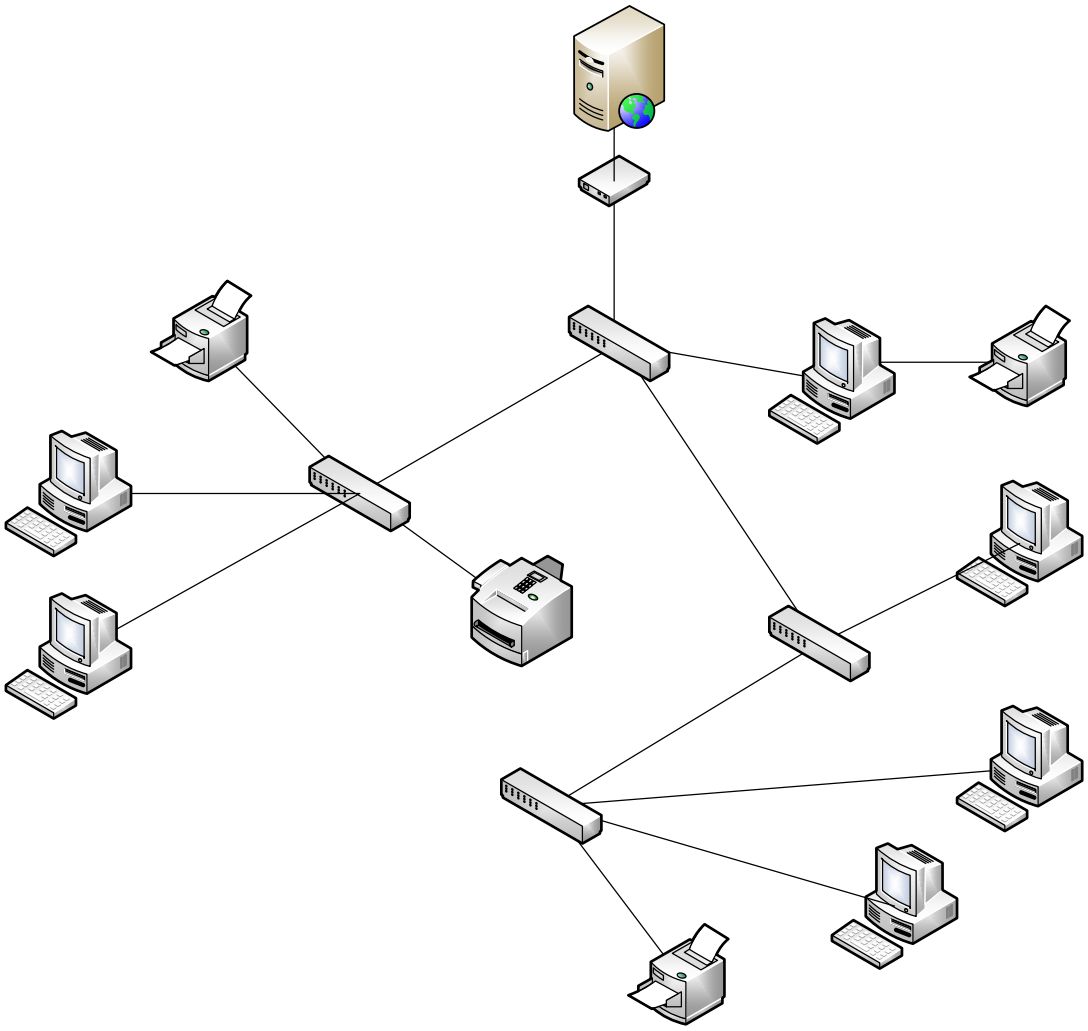
Jako antivirové řešení je použito řešení od společnosti ESET ve verzi Endpoint Antivirus nebo starší verzi NOD32 Antivirus Business Edition.

V organizaci je k práci používáno celkem 13 počítačů, kde na dvou je provozována především Vema, na dalších třech jídelna a zbytek používá vedení školy a pedagogičtí pracovníci pro přípravy.

Stáří počítačů je od 5 měsíců po asi 11 let. Kde zejména starší sestavy jsou na hranici minimální konfigurace pro provoz MS Office a internetového prohlížeče, jehož volba je ponechána na preferencích uživatele. Proto na některých sestavách není odezva systému vždy dostačující. S obnovou počítačových stanic se začalo před asi třemi roky. Upouští od modelu 1 PC = 1 tiskárna, zejména pro vysoké náklady na tisk na malých zejména inkoustových tiskárnách. Kanceláře jsou na budovách rozmístěny různě a většinou i dále od sebe. Proto jsou používány síťové tiskárny nebo je použita alespoň možnost jejich sdílení.

Jak již bylo naznačeno, tak pracoviště nejsou propojena, komunikace mezi pracovišti je možná pouze po telefonu a výměna souborů probíhá buď osobně, nebo e-mailem. Pracoviště Lidická a Bílkova jsou připojeny k internetu od společnosti MAXPROGRES Telco, s.r.o., s rychlostí připojení až 50 Mb/s v obou směrech, pracoviště Na Dolech je připojeno přes ADSL od společnosti GTS Czech s rychlostí 8/0,5 Mb/s

Zapojení do sítě je realizováno pomocí přepínačů a směrovače s modemem do sítě internet, na pracovišti Na dolech je použit jen modem, a k němu jsou připojeny počítače. Na následujícím obrázku je znázorněno ilustrační schéma zapojení pracoviště Lidická



Obrázek 13 – Ilustrační schéma zapojení sítě

Podklady pro následující dvě kapitoly byly získány vyplněním dotazníků na portále ZEFIS. (www.zefis.cz)

2.3 Analýza metodou HOS 8

Při analýze byl zjištěn následující stav úrovní:

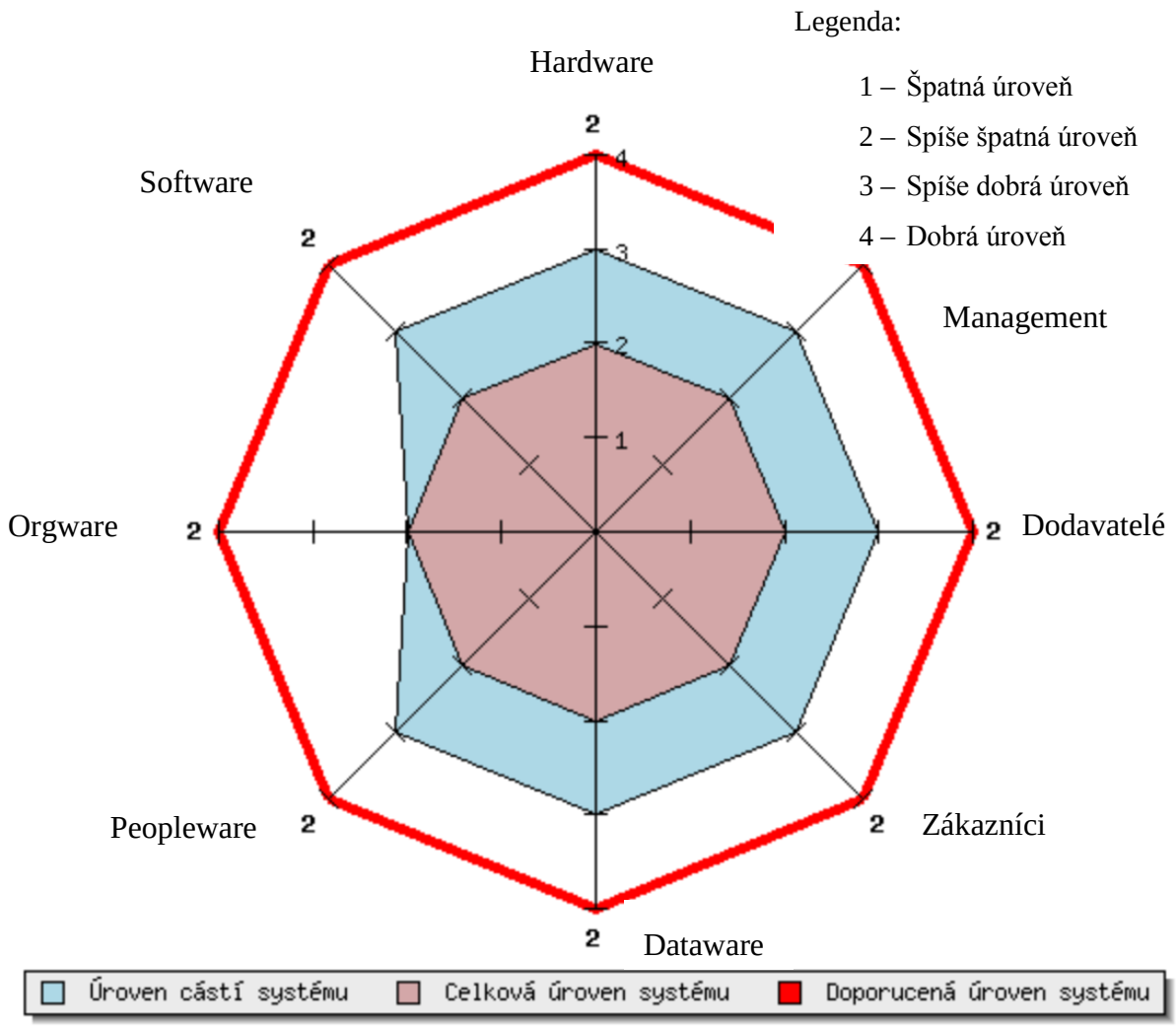
Tabulka 1 – Stav úrovní jednotlivých oblastí

Hardware	spíše dobrá úroveň
Software	spíše dobrá úroveň
Orgware	spíše špatná úroveň
Peopleware	spíše dobrá úroveň
Dataware	spíše dobrá úroveň
Zákazníci	spíše dobrá úroveň
Dodavatelé	spíše dobrá úroveň
Management IS	spíše dobrá úroveň

Jak je z tabulky vidět není úroveň informačního systému až tak špatná, Nejnižší úroveň je v oblasti Orgware, což jsou pravidla pro provoz IS. Tento systém můžu považovat za vyvážený, protože splňuje podmínku této metody tj.: Za vyvážený IS informační systém se považuje ten, ve kterém se vyskytují pouze dvě sousední hodnoty, přičemž jedna hodnota *u* zde musí převažovat.

Ovšem na základě této metody je celková úroveň dána nejslabším článkem, tedy celková úroveň IS je spíše špatná.

Celkové hodnocení je znázorněno na následujícím obrázku.



Obrázek 14 – Znázornění úrovně systému

Doporučená úroveň informačního systému je dobrá. Celková úroveň posuzovaného systému je o 2 body nižší., a to kvůli oblasti Orgware, která dosáhla nejnižšího hodnocení.

2.3.1 Hardware

Při zkoumání této oblasti na základě odpovědí na otázky v metodě HOS bych doporučil pokračovat v pozitivním trendu obnovy techniky zejména nutnost vyměnit počítače jejichž stáří je 10 let, a jejichž výkon téměř nestačí ani pro provoz samotného operačního systému, přestože splňují minimální konfiguraci (tj. výkon procesoru – CPU, velikost operační paměti, a požadavky na diskový prostor a požadavky na grafický procesor). V oblasti nákupu hardware bych nepoužíval cestu vždy nejlevnějšího řešení, protože se může stát, že by toto zařízení bylo

nutné vyměnit dřív než by byla obnova plánovaná. Někteří uživatelé si již na nižší odezvu systému zvykli a přizpůsobili jí svoje pracovní tempo.

Rychlost sítě a stabilita hardware je pro účely organizace dostačující, poruchy v oblasti hardware se téměř nevyskytují.

Ochrana hardware je na dostačující úrovni, Počítače jsou po většinu pracovní doby pod dohledem, a mimo pracovní dobu v uzamčených prostorách vybavených elektronickým zabezpečovacím systémem (detekujícím pohyb nebo rozbití oken) napojeným na Městskou policii.

2.3.2 Orgware

Toto je nejslabší část systému v organizaci.

Nejsou definovány bezpečnostní pravidla informačního systému (která by měly definovat alespoň, zda má uživatel přístup na internet a kam, s jakými daty pracovat a zda má mít na počítači heslo, jeho délku složitost tj. jaké znaky by mělo obsahovat, a jak často by toto heslo měl uživatel měnit.). Zda může instalovat programy nebo měnit nastavení popř. zda může k počítači připojovat další zařízení. V neposlední řadě řešení ukončení přístupových práv po skončení pracovního poměru.

O práci s informačním systémem byly uživatelé většinou seznámení školením nebo se o dalších možnostech seznámili od více zručného uživatele. Naštěstí alespoň mají základní pud sebezáchovy a neklikají na podezřelá okna na internetových stránkách. Bylo by vhodné alespoň šířit právní povědomí o instalaci programů. Myslím, že vzhledem k velikosti organizace a fluktuaci zaměstnanců není příliš potřebné stanovovat pravidla pro zrušení přístupových práv. Většina zaměstnanců pracuje v organizaci již více než 10 let a nedochází tedy k jejich časté obměně. Občas jsou používaný pro firemní komunikaci i soukromé e-maily, kde firemní e-mail zrušit nebo přesměrovat organizace po odchodu zaměstnance může, ale data která mohou zůstat na soukromém e-mailu, tam zůstanou. Pokud jsou nějaká pravidla definována, tak o nich není žádný písemný záznam a jsou šířena pouze neformální cestou.

Mnoho z těchto nedostatků vyplynulo při sloučení, kdy dosud ještě nebylo příliš nutné využívat počítače a po sloučení se elektronická komunikace značně rozšířila. Nicméně zavedení některých směrnic a jejich kontroly, by v určitých případech mohlo vést k nárůstu již tak velké administrativní zátěže.

Bylo by vhodné alespoň vypracovat směrnici o používání e-mailů a zásady hesel a přístupu k počítačům vůbec.

2.3.3 Software

Tato oblast zkoumá, zda software plní většinu funkcí, které uživatelé potřebují.

Informační systémy používané v organizaci, mají podle názorů jejich uživatelů, většinou hlášení, které neposkytují přímo návod k řešení problému. Vyhledání této chyby také není vždy jednoduché.

Jinak jsou uživatelé celkem spokojení s grafickým vzhledem IS a jeho členěním, i rozhraním pro zadávání vstupních údajů, stejně tak pokrývá alespoň 90 % jejich potřeb a má jednotný styl ovládaní. Celkově jsou uživatelé spokojeni a informační systém vyhovuje jejich potřebám.

2.3.4 Peopleware

Pracovníci absolvují pro práci s IS školení, zpravidla jsou poté v ovládání samostatní a pomoc potřebují pouze při řešení nestandardních situací. Též mají zaměstnanci možnost zúčastnit se dalších školení pro rozvíjení jejich schopností.

Zastupitelnost zaměstnanců na jejich pozicích většinou možná je V případě dlouhotrvající pracovní neschopnosti některé vedoucí stravování, může její úkoly dočasně zpracovávat jiná, popřípadě pokud není práce zvlášť termínovaná, počká.

Nižší zastupitelnost zaměstnanců je u účetní a ekonomky zpracovávající mzdy. Účetnictví má čtvrtletní uzávěrky, takže se většina agendy dá dohnat, nepočkají například úhrady faktur, ty může uhradit někdo jiný. Mzdy musí být zpracovány vždy v termínu, neboť termín výplaty je dán v pracovní smlouvě a hovoří o něm i Kolektivní smlouva.

Řešením této situace by mohla být práce z domova pomocí vzdáleného připojení nebo proškolení účetní do mezd, protože je v organizaci zpracovávala před sloučením organizace.

2.3.5 Dataware

Tato oblast se zaměřuje na to, jak je v organizaci nakládáno s daty. To je, jestli jsou chráněna i proti internetovým hrozbám nebo zálohována.

Uživatelé nemají formální zodpovědnost za data. Tato odpovědnost je dána spíše neformálně a vyplývá z jednotlivých funkcí. Není prováděna automatická záloha dat. Potřebná data by si měli zaměstnanci zálohovat sami alespoň na vyměnitelné médium jako je USB- flash disk nebo druhý pevný disk. Občas se stává, že vytvořená záloha je umístěna na stejném disku, pokud je vůbec nějaká provedena. Obnova ztracených dat může trvat občas více než týden, protože zálohování zaměstnanec jinam provede občas jen jednou za pár měsíců, obnova těchto dat proto může zabrat i více než 14 dnů. V organizaci existuje směrnice pro archivaci, která řeší jen to, co je archivováno a na jak dlouho. Směrnice pro zálohování neexistuje. Jen na jednom počítači probíhá automatická záloha pomocí diskového pole RAID 1. Data, které podléhají povinné archivaci, jsou pouze v papírové podobě.

Ochrana proti hrozbám z internetu probíhá pomocí vestavěného firewallu systému Windows a antivirového programu zmíněného výše.

2.3.6 Dodavatelé

Zde se řeší, kdo má na starost provoz IS

Pro podporu se systémem Vema se organizace obrací přímo na společnost Vema, které je pravidelně placen udržovací poplatek za aktualizace, prodloužení licence a základní pomoc. Komunikace probíhá většinou přes Call centrum, popřípadě e-mailem nebo vzdáleným přístupem s řešitelem problému. Pro systém Evidence jídelny je pravidelně jedenkrát ročně placena částka za aktualizaci systému a podporu. Většina požadavků se řeší operativně přes vzdálenou pomoc, přímo před očima zaměstnance a po telefonu.

Výměnu tonerů a běžně vyměnitelných součástí tiskáren si organizace dělá sama. Provádí ji jeden více zručný zaměstnanec na každém pracovišti. Instalaci software provádí většinou externí pracovník zpravidla do jednoho dne od požádání. Složitější zásahy poté řeší externí firma, která je místní a reaguje po zavolání většinou do jednoho dne. Organizace má s firmou dobré vztahy.

Co se týče doby mezi požadavkem a jeho vyřešením, jsou uživatelé většinou spokojení.

Provoz e-mailů má na starost zřizovatel.

2.3.7 Management IS

Vzhledem k zaměření organizace plní informační systém spíše podpůrnou úlohu. Vedení organizace by mělo vypracovat nebo nechat vypracovat směrnici o provozu a bezpečnosti pro informační systém a poté kontrolovat její dodržování. Organizace též nemá zpracovánu informační strategii, což v podstatě ani nepotřebuje. Jen bych doporučoval postupně vyměňovat zařízení a též software, nejlépe tak, aby stáří nepřesahovalo cca 8 let. O obměně zařízení se v organizaci rozhoduje podle volných finančních prostředků.

2.3.8 Zákazníci

V případě této organizace je pojem zákazník míněn jako uživatel informačního systému. Organizace nemá zpracovánu informační strategii. Některé počítačové vybavení, jak již bylo zmíněno, plně nepřispívá k dostatečně rychlým odezvám na požadavky zákazníků, což může vést ke snížení efektivity práce.

Pravidla o nakládání s citlivými popř. osobními údaji jsou řízena zákonem 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

Vzhledem, k tomu, že jsou využívána hotová řešení, není příliš možností ke změně. Návrhy uživatelů systému Evidence jídelna jsou občas brány v potaz jeho výrobcem a zapracovány do další verze.

2.4 Průzkum efektivnosti IS pomocí ZEFIS

Pro tento průzkum, bylo vyplněno celkem 6 dotazníků od zaměstnanců, kteří pravidelně pracují s informačním systémem. Pomocí portálu ZEFIS jsou v této oblasti rozděleny otázky do oblastí:

- Váš informační systém,
- Vaši zaměstnanci,
- Úroveň podpory,
- Úroveň řízení,
- Efektivnost IS,
- Bezpečnost IS,
- Chápaní IS jako služby.

Podle této metody byl vyplněn dostatečný počet dotazníků pro posouzení celé organizace. Její výsledky mohou být vztaženy na celou organizaci, i když může dojít k menším a málo pravděpodobným odlišnostem.

Údaje vyplněné o společnosti jsou věrohodné, všichni respondenti se shodli na základních údajích.

Tabulka 2 – Základní údaje o organizaci

Velikost vaší firmy	50-99	6/6
Oblast podnikání	Vzdělávání	6/6
Země	Česká republika	6/6
Orientační počet počítačů	10-49	6/6

V této metodě jsou pouze relativně velké intervaly, takže pří celkovém počtu 13 počítačů spadá organizace do kategorie 10-49.

Ve vyhodnocení jsou používány pouze tři nejčastější odpovědi, proto se součet procent nemusí rovnat 100.

Vzhledem k velikosti organizace byly posuzovány všechny informační systémy, jež jsou používány.

2.4.1 Informační systém organizace

Tato část řeší, jaké mají zaměstnanci povědomí o IS, který je používán. Proto na otázku jaký informační systém používáte, odpovědělo 66 % že systém je malý, 16 %, že používá jen kancelářský balík a 16 % že neví, jaký používá systém.

V otázce týkající se stáří odpovědělo 50 % že je stáří 3-5 let, 16% nevědělo a 16 % že 1-3 roky. Tato otázka nevypovídá o celkovém stáří systému, protože se zde střídají všechny typy systémů, kde Vema a Jídelna jsou pravidelně aktualizovány na nové verze, kancelářské balíky byly zmíněné výše a nejčastěji jsou staré více než 5 let.

V otázkách týkajících se silných a slabých stránek informačního systému byly některé odpovědi protichůdné. Nejčastější odpovědi jsou v následující tabulce.

Tabulka 3 – Silné a slabé stránky IS

Silné stránky			Slabé stránky	
technika	50 %		Programové vybavení	37 %
Přesnost a úplnost dat	12 %		Technika	25 %
Žádné (neuspokojivé)	12 %		Rychlost odezvy	25 %

Tyto odpovědi odrážejí již dříve zjištěné odlišnosti zejména v používaných počítačích, kde ti uživatelé, kteří používají nový, jsou spokojení a ti co mají staré a starší programy jsou poté nespokojení.

Všichni pracovníci v průzkumu pracují v organizaci déle než tři roky. Jejich vztah k počítačům je znázorněn v následující tabulce:

Tabulka 4 – Vztah uživatelů IS k PC

Neutrální, umím s nimi pracovat na požadované úrovni, ale nemám o ně velký zájem	50 %
Negativní, nemám je rád/a a mám problémy s nimi pracovat	33 %
Dobrý, umím s nimi dobře pracovat, využívám je ve většině případů, kdy to povaha práce/zábavy umožňuje	17 %

Jak je z tabulky patrné, uživatelé nemají příliš kladný vztah k PC, což se může odrazit na negativním postoji k jakékoliv změně v oblasti informačních systémů. Dá se předpokládat i jejich nižší znalost v této oblasti, což může znamenat i plné nevyužívání možností IS.

Pracovníci, kteří se zúčastnily průzkumu, informační systém používají v 50 % několikrát denně, ve 33 % případech většinu pracovní doby a v 17 % případů několikrát týdně. V této otázce se odráží i předchozí otázka a to převládající negativní nebo neutrální vztah k PC a jejich využívání.

Všichni účastníci průzkumu se shodli, že organizace podporuje jejich další vzdělávání.

2.4.2 Podpora

Tato oblast zkoumá, jakou podporu v práci s informačním systémem mají zaměstnanci k dispozici a dále, jak jsou s ní spokojeni.

S podporou je spíše spokojeno 16 % zaměstnanců a zbytek označil tuto podporu jako průměrnou. Tato podpora v sobě odráží technickou i uživatelskou podporu. Většinu podpory

zajišťuje externí firma a jsou využívána hotová řešení. Podpora je uskutečňována převážně po telefonu. Zaměstnanci mohou mít pocit neosobního jednání a zejména vzhledem k postoji k zařízením, které využívají, nemusí být plně schopni popsat problém (taky je pracovník na technické podpoře nemusí plně pochopit) a tedy mají pocit, že je podpora na nižší úrovni.

V této otázce je započítána i výměna tonerů a jiného spotřebního materiálu. Toto si provádějí zaměstnanci svépomocí.

Uživatelská podpora, která se týká pomoci s informačním systémem a daty, je podle výsledků prováděna z 84 % někým z kolegů, který není přímo pracovníkem útvaru IS. Zbytek zajišťuje externí pracovník z jiné firmy.

Doba opravy (závady)

je doba, jak dlouho musí uživatel čekat na vyřízení požadavku. Tyto opravy jsou vyřizovány podle toho, jak moc uživatel potřebuje počítač ke své práci, aby pokud možno nedošlo ke snížení produktivity nebo znemožnění jeho práce. Účastníci průzkumu v této oblasti odpověděli:

- 2-5 dnů 33%
- 1-2 dny 33%
- méně než 1 den 33%

Doba instalace nebo změny programů

Tato podpora není tak důležitá jako technická podpora počítačů. Přesto je na tom tato oblast trochu lépe. Respondenti vypověděli, že v 50 % je tato doba 1–2 dny a v 16 % méně než jeden den a v 16 % 2 – 5 dnů.

Na druhou stranu je oblast podpory možno považovat i za dobrou, vzhledem k tomu, že v organizaci není nikdo, kdo by se přímo podporou zabýval.

2.4.3 Úroveň řízení

Samostatný pracovník starající se o IT vzhledem k velikosti a zaměření organizace není. Tato funkce je konsolidována s jinou. Pracovník má na starosti pouze správu informací o zařízeních a licencí k používaným programům. Informační systémy jsou brány jako podpůrné, proto není ani informační strategie. Do IS je zpravidla investováno podle volných finančních prostředků. Co se týče toho, jaké informační systémy mají zaměstnanci používat, je toto dáno jejich pozicí. Stejně tak data, která a kdy se mají do systému vkládat, jsou dána jen pozicí. Přímá pravidla pro práci se systémem nejsou definována.

2.4.4 Efektivnost informačního systému

V této oblasti je zkoumáno, zda byly vynaložené prostředky adekvátní, jak moc je pro pracovníky IS důležitý, popřípadě jestli by mohl v některých oblastech více pomoci.

Na otázku, **zda by mohli zaměstnanci vykonávat svoji práci i bez IS**, jsou odpovědi v následující tabulce.

Tabulka 5 – Možnost vykonávat práci bez IS

Částečně, s velkými obtížemi	50 %
Ano, bez potíží	16 %
Ano, s malými obtížemi	16 %

Různé mínění v této oblasti kde si asi 32 % zaměstnanců myslí, že by zvládlo vykonávat práci bez IS vůbec nebo pouze s minimálními obtížemi, souvisí s jejich pozicí a náplní jejich práce. Tam informační systém plní pouze podpůrnou funkci.

Podobné mínění je u účastníků i v otázce jestli by **bez IS mohla organizace existovat**. Zde si 50 % myslí, že ano s velkými obtížemi a 16 % bez větších obtíží. 16 % odpověď na tuto otázku nezná nebo nedokáže posoudit.

Podle 50 % zaměstnanců by změna IS nemohla vést ke zlepšení jejich práce, zde se naskýtá otázka, jestli by opravdu nemohla vést ke zvýšení produktivity práce nebo vzhledem k jejich negativnímu postoji k IT mají také negativní postoj k jakékoliv změně v této oblasti. 33 % si myslí, že změna IS by měla jen velmi malý vliv na pracovní výkon respektive jeho zvýšení.

V oblasti **školení** se zkoumá, zda byli uživatelé školeni nebo ne a jaký přínos toto školení mělo, nebo zda by další školení mělo pro ně další přínos. Všichni absolvovali nějaké školení. Částečný přínos mělo toto školení pro 83 % respondentů, zbytek nevěděl, jestli školení pro ně přínos mělo. V mínění jestli by mělo proběhnout další školení si myslí 66 %, že další školení nepotřebují nebo jej spíše nepotřebují. Takže mají pocit, že to co ze systému znají, je pro ně dostačující.

2.4.5 Bezpečnost informačních systémů

Jisté nedostatky v této oblasti již naznačovaly výsledky v metodě HOS.

V otázce, zda existují bezpečnostní pravidla a zda je pracovníci dodržují a vedení vyžaduje jejich dodržování, všichni zúčastnění odpověděli, že nemají žádná pravidla, nebo o nich nevědí.

V části přístupu do počítačové sítě, ať již vlastní zaměstnanci nebo veřejnost (tj. zda si mohou připojovat svoje soukromá přenosná zařízení do podnikové sítě), což může zvyšovat riziko pro počítačovou síť. Zejména kvůli možnému nižšímu zabezpečení těchto zařízení a umožnění případného útoku na síť viry, špionážními programy a podobně.

V těchto dvou částech jsou vyrovnané odpovědi, kde polovina respondentů říká, že se dá bez problémů připojit a druhá, že neví a nikdy toto nepotřebovali.

Zabezpečení v tomhle ohledu není. Vzhledem k tomu, že v organizaci nejsou užívány bezdrátové sítě, je počet míst, kde se dá připojit, limitován zejména počtem zásuvek pro místní síť LAN nebo počtem jejich kabelů.

V úrovni vnímání rizik v otázce jak by uživatelé reagovali v případě možného ohrožení jejich počítače útočícím virem, špionážním programem či podobnou závadnou aplikací by pracovníci na žádost o povolení přístupu neznámého programu na jejich počítač (byť se tvářícího neškodně a legitimně) reagovali. Všichni odpověděli, že by zavřeli okno prohlížeče.

V části zálohování a otázce zda mají pracovníci na svých počítačích uložena data a jak jsou chráněna proti případnému poškození nebo zničení (jakým způsobem jsou zálohována). Odpověděli následujícím způsobem.

Tabulka 6 – Způsob zálohování

Sám	50 %
Nikdo, ale na mém počítači jsou soubory a data, které vytvářím a používám ke své práci	16 %
Zálohování mého počítače probíhá automaticky	16 %

V případě automatického zálohování, je pravděpodobně odpovědí myšleno použití diskového pole, kde jsou data ukládaná na jeden disk a zároveň i na disk druhý. Naskýtá se

otázka, kam který pracovník zálohu ukládá, to je zda leží ve stejném počítači a na stejném disku nebo je umístěna jinde.

V případě otázky jaký by byl dopad v případě jejích poškození tedy, jak dlouho by trvala jejich obnova, odpovědělo 33 %, že by jim obnova trval 2 – 5 dnů, dalších 33 % odpovědělo, že by byla zničena všechna jejich práce a 16 % odpovědělo, že by obnova trvala více než 5 dnů.

Výsledky této části vedou k závěru, že data sice zálohována jsou, ale nejlépe na stejném počítači a disku. Je také otázkou, jak často kdo zálohuje. Zdá se, že jen minimum záloh je ukládáno na jiná místa.

Na otázku vnímání bezpečnostní politiky, tedy zda uživatelé používají hesla a jak je chrání, byly následující odpovědi:

- Pamatuji si je, odpovědělo 50 %
- Hesla nepoužívám, odpovědělo 16 %
- Heslo mám zapsáno někde poblíž počítače, odpovědělo 16 %

Tento dotazník ovšem neřešil to, jak jsou tato hesla složitá a kolik mají alespoň znaků. S přihlédnutím k předchozím částem a zejména vztahu uživatelů k PC a IS usuzuji, že hesla budou spíše jednodušší.

Na otázku týkající se ztráty dat, zejména možnosti krádeže zařízení, jsou odpovědí v následující tabulce

Tabulka 7 – Následky ztráty dat

Žádný, data na počítači jsou chráněna přihlašovacím jménem a heslem	50 %
Mírný, prozrazení firemních dat na tomto počítači nemůže firmě způsobit vážnější problémy	34 %
Střední, prozrazení firemních dat na tomto počítači může firmě způsobit problémy	16 %

Odpovědi v této tabulce reflektují předchozí části, tj. jak jsou data chráněna v tomto případě a zda jsou hesla nebo nejsou.

Všichni zaměstnanci mají možnost přístupu na internet, který není nijak limitován. Ve většině případů je tento přístup nutný. Všichni zúčastnění jsou si možnosti přístupu vědomi.

Na otázku, zda uživatelé mohou připojit k počítači externí paměťová média (disky, flash paměti) a kopírovat a odnášet tak případně firemní data, případně infikovat počítače organizace závadnými programy, a tím zvyšovat riziko zneužití dat a bezpečnosti, odpovědělo 83 % dotázaných ANO a 17 % NE.

Otázka, zda uživatelé mohou instalovat sami na počítače organizace programy. Pokud uživatel nainstaluje nelegální programy, odpovědnost je i na straně organizace. Odpověděly všichni ANO, tj. všichni jsou si této možnosti vědomi a mohou tím zvyšovat rizika bezpečnostní ale i právní.

Chápání informačního systému jako služby. Zkoumá se, zda pracovníci chápou informační systém jako službu, podpůrný proces své práce, nebo jako celkovou součást svých procesů. Toto chápání je důležité pro úvahy o možném outsourcingu informačního systému, jeho části či podpory pracovníků.

V otázce, zda pracovníci chápou IS jako službu a jestli by taková služba mohla být zajišťována externí firmou, tedy tento systém by byl pronajímán a nebyl provozován v organizaci, si 50 % myslí, že spíše ano, 16 % spíše ne a 34 % neví. Nevědomost v této oblasti je způsobena tím, že pracovníci nemají zkušenosti s outsourcingem, kde tak odpověděli všichni a zda je nějaký proces zajišťován outsourcingem odpověděli pracovníci 50 % ne a 50 % nevím.

2.5 Analýza rizik a návrhy na jejich odstranění

V této kapitole budou posuzována rizika týkající se informačního systému. Jako hlavní podklad k tomuto budou použité předchozí analýzy a hrozby s riziky zjištěné při návštěvě organizace.

2.5.1 Analýza rizik

Obecný postup analýzy rizik:

- Identifikace aktiv (tj. co se bude posuzovat),
- Stanovení hodnoty aktiv (jaký bude dopad při jejich ztrátě nebo poškození popř. zničení na organizaci),
- Identifikace hrozeb a slabin (jaké události mohou poškodit aktiva organizace, popřípadě určení míst, která mohou umožnit působení hrozeb.),
- Stanovení míry závažnosti hrozeb a míry jejich zranitelnosti (určení pravděpodobnosti a míry závažnosti),

Tato první část je nazývána jako identifikace rizik.[38]

Druhá část se skládá z:

- Posouzení dopadů, pokud dojde k realizaci hrozby na konkrétní aktiva
- Stanovení úrovně rizika
- Rozhodnutí, jestli jsou rizika akceptovatelná nebo ne podle jejich úrovně. Pokud jsou rizika neakceptovatelné realizovat vhodná opatření ke snížení jejich významnosti. [38]

V předcházejících částech byla zjištěna rizika, která jsou zejména bezpečnostního charakteru, kde některá vyplynula z oblasti Orgware (nebyla tu definována žádná bezpečnostní politika) a oblasti bezpečnosti IS.

Příklad zjištěných rizik:

- Bezpečnostní riziko, kdy je možné téměř volné připojování cizích zařízení do sítě, což může umožnit útok na síť viry, špionážními programy apod. z důvodu, že tato zařízení mohou být méně chráněna.
- Riziko ztráty popřípadě zneužití dat a tím pádem i ohrožení bezpečnosti**,** které může být vyvoláno nezálohovanými daty a riziko zneužití dat způsobené pracovníky tím, že mohou připojovat přenosná zařízení a na těchto zařízeních poté odnášet firemní data, kde toto zařízení mohou později ztratit.

Z přenosných zařízení vyplývá i riziko podobné jako u počítačové sítě a to je možnost infikování počítače závadnými programy.

- možnost instalace programů na počítače jejich uživateli
- rizika vyplývající z absence jakékoliv bezpečnostní politiky, kde poté není možnost vyvodit důsledky z jakéhokoli jednání týkajícího se IS

[38] SMEJKAL Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 4., aktualiz. a rozš. vyd. Praha: Grada, 2013, 483 s. Expert (Grada). ISBN 978-80-247-4644-9. str. 95, 96

Pro analýzu rizik je použita metoda dle ČSN ISO/IEC 27005:2008 [39] (kde pro vyhodnocení je použita pravděpodobnost s jakou scénář nastane, je na stupnici od nepravděpodobná po velmi vysoká (stupnice 1-5, kde nepravděpodobná je 1, až velmi vysoká je 5). Dopad od zanedbatelný po velmi závažný (opět stupnice 1 – 5, kde 5 je velmi závažný). Významnost rizika je vyjádřena jako součet pravděpodobnosti a jeho dopadu, může tedy nabývat hodnot od 2 do 10. Pro hodnocení dopadu je stupnice rozdělena na 3 časti: Nízká významnost: dopad na organizaci nebo finance je zanedbatelný; zvýšená - dopad na chod organizace nebo finance může být více patrný; vysoká významnost: dopad organizaci může mít velký nepříznivý vliv zejména finanční. Podrobný popis je uveden v následujících tabulkách.

Tabulka 8 – Stupnice pravděpodobnosti [39]

pravděpodobnost

parametr	popis	hodnota
nepravděpodobná (0 % – 5 %)	výskyt jevu je nepravděpodobný	1
Nízká (5 % – 20 %)	jev je málo pravděpodobný	2
střední (20 % – 50 %)	jev se vyskytuje příležitostně	3
vysoká (50 % – 70 %)	jev se vyskytuje často	4
velmi vysoká (70 % – 100 %)	jev se vyskytuje velmi často	5

Tabulka 9 – Stupnice dopadu

dopad	hodnota
zanedbatelný	1
malý	2
střední	3
závažný	4
velmi závažný	5

Tabulka 10 – Významnost

Významnost rizika	
2 – 4	Nízká
5 – 6	Zvýšená
7 – 10	Vysoká

[39] SMEJKAL Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 4., aktualiz. a rozš. vyd. Praha: Grada, 2013, 483 s. Expert (Grada). ISBN 978-80-247-4644-9. str. 133 – 135

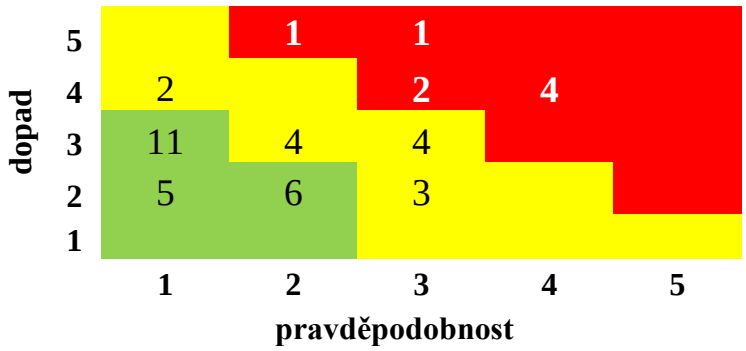
V následující tabulce jsou zaznamenány zjištěné hrozby a rizika, které mohou nastat u posuzovaného informačního systému.

Tabulka 11 – Hodnocení rizik

č.	**hrozba**	**riziko**	**pravděpodobnost**	**dopad**	**významnost**
1	požár, živelní pohromy	ztráta dat nebo jejich poškození	1	4	5
2	opotřebení paměťových médií nebo HW		3	3	6
3	výpadek proudu		2	2	4
4	kolísání proudu		2	2	4
5	chyba při přenosu popř. předčasné odpojení zařízení		2	2	4
6	nedostatečné zálohování		4	4	8
7	selhání IS		1	3	4
8	neúmyslné jednání uživatele IS		3	3	6
9	vniknutí do objektu		1	3	4
10	úmyslné jednání uživatele IS		1	2	3
11	úmyslné lidské hrozby pro IS	Odcizení dat	1	2	3
12		poškození HW	1	2	3
13		instalace nelegálních programů	2	5	7
14		poškození nebo smazání dat	2	3	5
15		instalace nepřátelského programu	1	4	5
16	neúmyslné lidské hrozby	chyby a zapomenutí	2	2	4
17		vymazání souboru nebo dat	3	2	5
18		nehody kdy dojde k poškození HW, sítě	3	2	5
19		instalace nelegálních programů	3	5	8
20		připojení nedostatečně zabezpečeného zařízení do sítě (škodlivý kód)	3	4	7
21		instalace nepřátelského programu	3	3	6
22	destruktivní útok na data	omezení dostupnosti systému	1	3	4
23	selhání HW nebo paměťových médií		2	3	5
24	výpadek připojení k internetu		2	2	4
25	požár, voda		1	3	4
26	chyba při údržbě		1	3	4
27	přírodní pohromy		1	3	4
28	selhání SW		1	3	4
29	nedostatečné HW vybavení	neefektivní práce	3	2	5

č.	hrozba	riziko	pravděpodobnost	dopad	významnost
30	nižší odezva systému	neefektivní práce	3	3	6
31	vniknutí do objektu	odcizení dat	1	2	3
32		odcizení HW a dat	1	3	4
33		poškození dat prostředí nebo Hardware	1	3	4
34	nechráněné úložiště	krádež nebo neoprávněné používání dokumentů	4	4	8
35	neodhlášení se od počítače		2	3	5
36	nepřiřazená přístupová práva		2	2	4
37	odcizení pracovní stanice		1	3	4
38	ztráta paměťového zařízení		4	3	7
39	žádná nebo nechráněná hesla		1	2	3
40	chybějící směrnice	nedostatečné zálohování	4	4	8
41		zmizení PC	1	3	4
42		omezená přístupnost k datům	2	3	5
43		nemožnost vyvedení zodpovědnosti	4	4	8

V následujícím grafu je znázorněna matice rizik, včetně četnosti jejich výskytu, kde žlutě jsou znázorněna zvýšená významnost rizika, červeně vysoká významnost rizika a zeleně nízká významnost.



Graf 1 – Součtová matice rizik

V následující kapitole se bude návrh řešení pro zlepšení stávajícího stavu a především pro eliminaci rizik a zejména hrozeb, které je způsobují, jsou to rizika s hrozbami znázorněné v předchozím obrázku v červené oblasti a v tabulce 11 hodnocení rizik s významností 7-10.

2.5.2 Návrhy řešení

Pro oblast Orgware navrhuji stanovit směrnici pro používání ICT a stanovení odpovědnosti za svěřená aktiva. Směrnice by měla obsahovat základní pravidla pro:

- Používání emailů:
  - K čemu je používán,
  - Jaké emailové účty se používají pro komunikaci v organizaci a mimo ni.
  - Jaká data se smějí posílat přes e-mail.
- Používání IT definující
  - Jaké zařízení je pracovník oprávněn používat,
  - Omezení používání prostředků zejména pro plnění pracovních povinností,
  - Zákaz instalace jiných programů než jsou nainstalovány,
  - Zákaz poskytnutí softwaru jinému uživateli (jak uvnitř tak vně organizace),
  - Určit pověřenou osobu, u které má zaměstnanec právo požádat o poskytnutí dalšího software, který nutně potřebuje pro svoji práci,
  - Určení odpovědnosti za vkládaná data,
  - Odpovědnost za svěřený majetek,
  - Způsob odnášení dat, jestliže to pozice umožňuje.
- Pravidla pro bezpečnost
  - Pravidla pro hesla obsahující alespoň nařízení mít na PC heslo, definovat požadavky na jeho délku a složitost popř. i frekvenci změny. Pravidla pro nakládání s hesly,
  - Postup při opuštění místnosti
  - Zákaz připojovat neschválená zařízení k PC nebo do sítě
  - Definici s nakládáním přidělených přenosných zařízení, pokud jim byla přidělena
- Závěrečná ustanovení definující alespoň
  - Osoby, které jsou oprávněny kontrolovat dodržování směrnice,
  - Jaké postihy mohou plynout při nedodržení směrnice,
  - Způsob uhrazení škody, která vznikla při nedodržení směrnice.

Některá další navrhovaná opatření se dotknou vynucování některých bodů této směrnice.

Pro omezení používání přenosných paměťových zařízení, jako jsou flesh disky a z nich vycházející rizika pro bezpečnost (spuštění škodlivého kódu, ztráta tohoto média a s tím související možnost ztráty citlivých údajů) je nutno omezit toto používání na minimum. Kompenzací k tomuto by mohlo být cloudové úložiště Microsoft OneDrive, získané pomocí plánu A2 pro vzdělávací instituce v OFFICE 365, který je zdarma a nabízí 25 GB úložného prostoru. Pokud bude uživatelům nainstalována aplikace, vytvoří se složka na ploše systému Windows, která je synchronizována s úložištěm. Tuto složku má poté uživatel k dispozici odkudkoliv, ať již pouze přihlášením na web OneDrive nebo opět pomocí aplikace na svém osobním PC. Aplikace jsou k dispozici i pro další operační systémy nebo mobilní operační systémy.

Je taktéž možné sdílení vybraných dokumentů a jejich řízení tak, že umožní přístup jen do určité složky nebo souboru jiným uživatelům, kteří buď mohou tento soubor pouze otevřít nebo i upravit, stejně tak pokud je povolen zápis do složky cizímu uživateli, může tento do dané složky přidávat sobory.

Toto řešení je možno použít i jako další cestu pro zveřejňování směrnic, které se týkají všech zaměstnanců. Pokud by si chtěli danou směrnici přečíst nebo prolistovat, mohou tak učinit kdekoliv a ne pouze na nástěnce v práci.

Součástí tohoto plánu je i základní webový nástroj pro vytváření nebo upravování dokumentů ve webovém prohlížeči. Stejně tak je součástí plánu ještě web podnikového intranetu, který by mohl být alternativou pro sdílení směrnic a možnost pořádat webové konference, kde mohou účastníci komunikovat prostřednictvím videa, sdílet obrazovky a zasílat rychlé zprávy. Pro řešení záležitostí, při kterých je nutný přechod některých zaměstnanců na jiné pracoviště, by tím odpadla doba, která je potřeba pro přesun zaměstnanců na pracoviště a zpět. Nevýhodou tohoto řešení je, že aplikace OneDrive pro Windows nepodporuje operační systém Windows XP a OS Linux. Z tohoto vyplývá, že uživatel by musel vytvořené soubory, které by chtěl nebo musel dopracovat doma nahrávat přes webový prohlížeč. Nebo by tu byla nutnost výměny zbývajících pracovních stanic alespoň u uživatelů, kteří občas potřebují dopracovat dokumenty doma.[40]

[40] http://office.microsoft.com/cs-cz/academic/porovnani-planu-office-365-education-FX103045755.aspx

http://office.microsoft.com/cs-cz/business/nastroje-office-365-pro-sdileni-souboru-a-online-spolupraci-FX102997013.aspx

http://windows.microsoft.com/en-us/onedrive/system-requirements

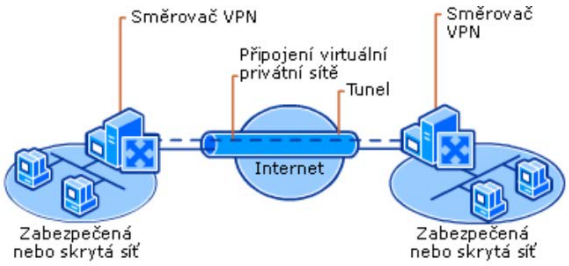
Pro řešení rizik souvisejících se zálohováním, přístupovými právy a vynucením některých zásad směrnice pro bezpečnost bych doporučoval následující řešení:

Propojení jednotlivých pracovišť pomocí VPN (Virtual Private Network) Virtuální privátní (soukromá) síť. Což je propojení mezi dvěma body přes veřejnou síť např. internet. Tedy např. mezi jednotlivými pobočkami podniku. Toto spojení je jako zabezpečený tunel v síti internetu, kde jsou data přenášena po ověření jednotlivých klientů. Toto ověření může být pomocí tzv. před-sdíleného klíče nebo pomocí certifikátu pro jednotlivá zařízení, popř. obojího. Data jsou šifrována tak, že v případě odposlechnutí jsou bez znalosti šifrovacího klíče, který znají pouze klienti, nečitelná. Je nutné dbát na dostatečnou délku tohoto klíče, protože v případě kratšího klíče roste riziko jeho prolomení a tedy možnost přečíst přenesená data.

Toto řešení umožní propojení jednotlivých pracovišť a možnost připojení pracovníků z domova. Taktéž umožní přístup k některým zdrojům, jako je možnost sdílení souborů z jednoho místa pro všechna pracoviště, a přístup k tiskárnám a dalším zařízením zapojeným v síti na jednotlivých pracovištích, což umožní zefektivnění výměny dokumentů.[41], [42]

Toto řešení umožní i vzdálenou pomoc uživatelům. Stejně tak by bylo možné v případě menší zastupitelnosti zaměstnance, připojit se a umožnit tak vykonat část práce z domova, aniž by bylo nutné proškolovat dalšího zaměstnance a toto školení u něj pravidelně opakovat, protože je pravděpodobné, že po třech měsících by práci za jiného zaměstnance nebyl schopen vykonat.

Stejně tak je toto řešení nedílnou součástí pro realizaci dalšího řešení k eliminaci rizik týkajících se zálohování a bezpečnosti.



Obrázek 15 – Schéma VPN [41]

[41] http://technet.microsoft.com/cs-cz/library/cc731954%28v=ws.10%29.aspx

[42] http://www.schindler-sys.cz/vpn-vzdalene-pripojeni/

Řešení pro zálohování a bezpečnost sítě

Navrhuji zavedení doménového řadiče, který umožní:

- Ověření uživatele
- Vynucení zásad pro hesla (nutnost jeho změny a požadavky na složitost
- Zařízení nebo počítači, který se připojí do sítě, sice bude přidělena adresa, ale nebude mít přístup k ostatním zařízením a službám sítě.
- Omezení uživatelských účtů pro jednotlivé uživatele, kterým bude znemožněno instalovat aplikace na počítače.[43]

Doménový řadič je v podstatě seznam, který obsahuje všechny informace o objektech v síti, tj. jak o počítačích, tak uživatelích a tiskárnách. Tyto informace shromažďuje a umožnuje tak uživatelům užívat jednotlivé objekty v síti. Zároveň umožní spravovat, k čemu mají uživatelé přístup a i tato přístupová práva uchovává.

Stejně tak pomocí tohoto budou omezena práva uživatelů a dojde k zamezení instalace programů. Dále také data z uživatelských složek budou umístěna na serveru, který bude chráněn proti výpadkům v elektrické síti, a zálohována. Budou tak více chráněna před zneužitím a odcizením. Proti výpadku napájecího zdroje má server jeden náhradní zdroj.

Zálohování dat bude prováděno na hlavním serveru pomocí diskových polí RAID. Dále počítám s možností provádění občasných záloh na server NAS, který bude sloužit pro další zálohování.

Jako ochranu před selháním hlavního řadiče domény, protože v případě jeho selhání, by došlo k nemožnosti se přihlásit k síti, navrhuji na jednom ze stávajících počítačů, který má dostatečný výkon, použít virtualizaci serveru, který bude také obsahovat řadič domény a převzal by služby v případě selhání hlavního serveru.

Protože na řadiči domény jsou ukládána i přístupová hesla, bude tato skříň umístěna v dostatečně zabezpečené místnosti.

Pro zajištění plné funkce bude nutné důkladně prozkoumat parametry služeb SLA, tj. úroveň poskytovaných služeb poskytovatelů připojení k internetu, protože v případě výpadku připojení k síti internet na některém z pracovišť, by nebylo též možné se připojit k serveru.

[43] http://blog.bcvsolutions.eu/stavime-domenovy-radic-a-dalsi-sluzby-site-uvod/

Smlouvy SLA by měly obsahovat informace o spolehlivosti, sankce za nedodržování parametrů a dobu, za kterou bude závada odstraněna.

S přihlédnutím k tomu, že některé místní síťové prvky v organizaci jsou umístěny u počítače, který má k dispozici krátkodobý zdroj napájení, by tyto sítové prvky k němu mohly být také připojeny, aby byl dostatečný čas pro přenos a uložení dat a nedošlo k jejich ztrátě při výpadku napájení.

Vzhledem k tomu, že toto navrhované řešení vyžaduje vyšší znalost informačních technologií, doporučuji pro následnou správu buď zaměstnání správce sítě na částečný úvazek, popřípadě důkladné proškolení některého zaměstnance aby vykonával kromě své běžné práce i práci správce sítě nebo uzavřít smlouvu se společností, která se touto problematikou zabývá a která by dohlížela na chod sítě a řešila některé požadavky uživatelů.

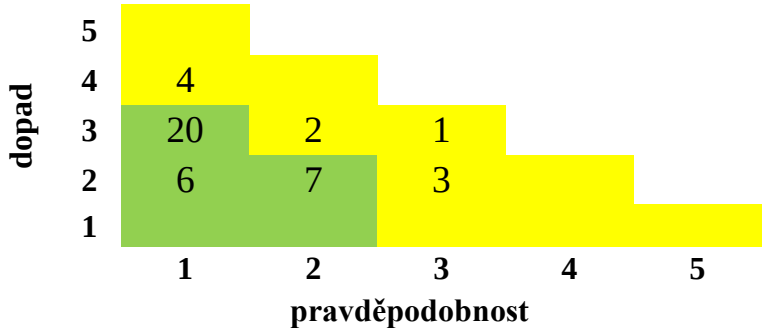
2.5.3 Vliv provedených opatření na identifikované hrozby a rizika

V následující tabulce jsou hrozby s riziky, u kterých došlo ke snížení vlivem navrhnutých opatření.

Tabulka 12 – Hodnocení rizik po provedení navrhovaných změn

č.	**hrozba**	**riziko**	**pravděpodobnost**	**dopad**	**nová významnost**
2	opotřebení paměťových médií nebo HW	ztráta dat nebo jejich poškození	1	2	3
6	nedostatečné zálohování	ztráta dat nebo jejich poškození	1	3	4
13	úmyslné lidské hrozby pro IS	instalace nelegálních programů	1	3	4
19	neúmyslné lidské hrozby	instalace nelegálních programů	1	4	5
20		připojení nedostatečně zabezpečeného zařízení do sítě (škodlivý kód)	1	3	4
21		instalace nepřátelského programu	1	3	4
34	nechráněné úložiště	krádež nebo neoprávněné používání dokumentů	1	4	5
35	neodhlášení se od počítače	krádež nebo neoprávněné používání dokumentů	1	3	4
36	nepřiřazená přístupová práva	krádež nebo neoprávněné používání dokumentů	1	2	3
38	ztráta paměťového zařízení	krádež nebo neoprávněné používání dokumentů	1	3	4
40	chybějící směrnice	nedostatečné zálohování	1	3	4
43		nemožnost vyvedení zodpovědnosti	1	3	4

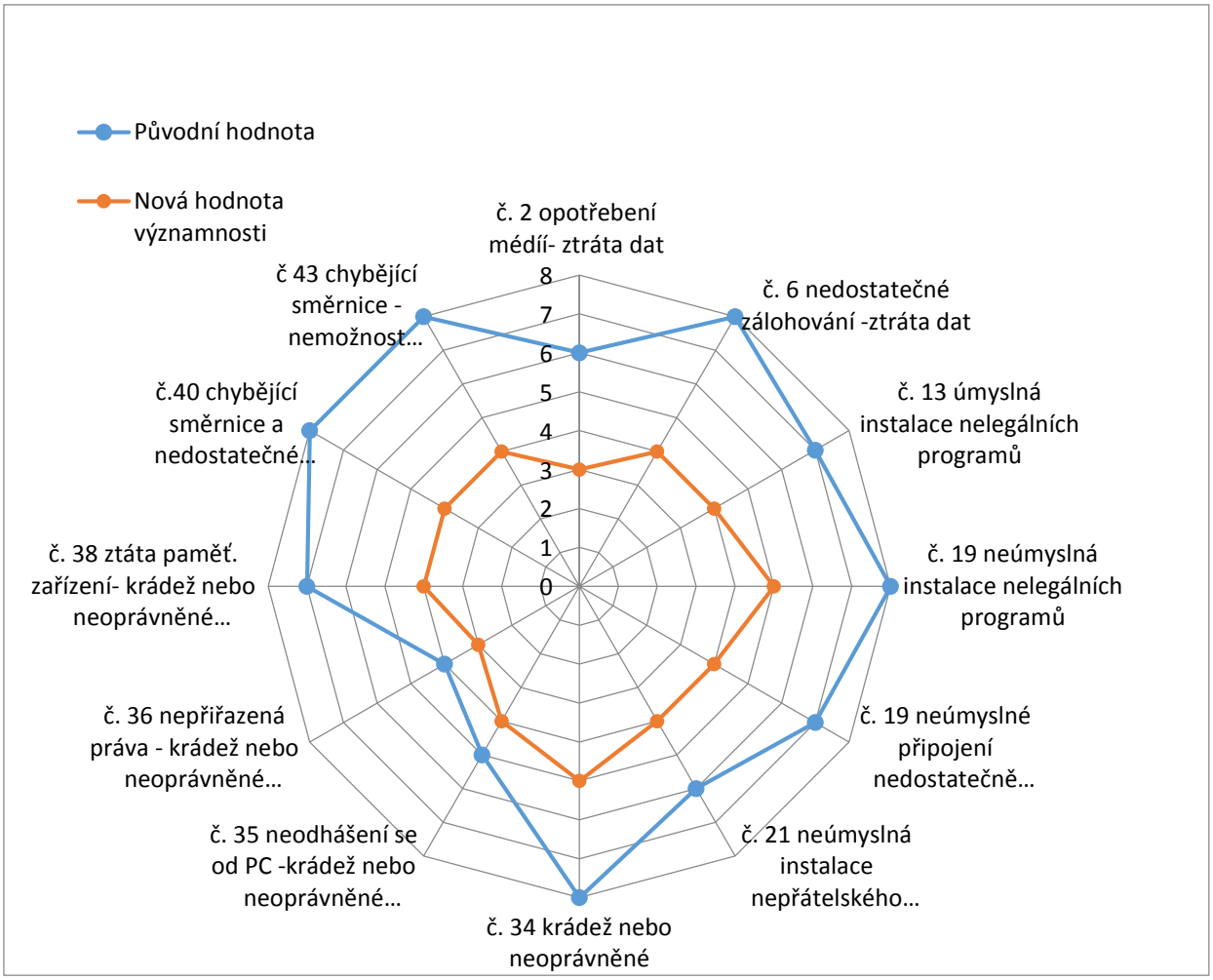
V následujícím grafu je součtová matice všech rizik, se zohledněnými riziky, u kterých došlo ke snížení vlivem navrhnutých opatření.



Graf 2 – Součtová matice rizik po provedených opatřeních

V následujícím grafu je znázorněna původní hodnota významnosti a nová hodnota významnosti, po provedených protiopatřeních.

Graf 3 – Znázornění původní hodnoty významnosti hrozeb a nové hodnoty významnosti po opatřeních



2.6 Náklady na navrhovaná opatření

V následující tabulce jsou náklady na navrhovaná opatření. Ceny jsou včetně DPH a v případě softwaru byly některé ceny v eurech a pro přepočet byl použit kurz České národní banky k 22. 5. 2014. V případě antivirového řešení ESET, je poplatek na 1 rok.

Ceny uvedené v tabulce byly získány z internetových stránek společnosti Alza.cz, pc.itek.cz, Eset.cz, D&COMM, Microsoft. Více viz. seznam literatury

Tabulka 13 – Náklady na navrhovaná opatření

Náklady na navrhovaná řešení	počet	Celkem v Kč
Rack GF6942 skříň		8 500
server IBM x3650M4		52 000
IBM 600 GB SAS 10000 RPM	2	24 594
MS Windows Server Standard 2012		5 729
Server 2012 User CAL	14	2 636
APC Smart-UPS C-1000VA- záložní zdroj	2	23 700
MS Windows 8.1 Pro upgrade EDU	2	3 348
instalace a zahoření serveru		5 000
zavedení doménového řadiče a VPN		17 000
Eset file security for Windows Server		2 091
MS Office 365 educatinon plán A2		0
Synology DiskStation DS214+		9 099
Western Digital Red 2000GB 64MB	2	4 998
VPN router CISCO RV320-K9-G5	3	15 420
Celkem		**174 115**

Tyto náklady na provedená opatření neobsahují trvale zvýšené náklady, které by mohly vzniknout při zvýšení úvazku zaměstnance, nebo části úvazku nového zaměstnance, popř. nákladů za externí služby týkající se správy sítě po těchto provedených opatřeních.

Ceny za software jsou nižší než standartní ceny na trhu, z důvodů slev pro vzdělávací instituce.

Tyto náklady předpokládají, že směrnice v této oblasti bude vypracována jako součást stávající práce. Tedy nevzniknou náklady na vypracování směrnice, která je navrhována v řešení.

V případě, že nebude k dispozici dostatek finančních prostředků, navrhuji alespoň vyřešit zálohování zakoupením 3 NAS serverů s nižší diskovou kapacitou, při zachování 2 disků v poli RAID na každé pracoviště. Tím lze snížit náklady na přibližně 72 000 Kč. Tím dojde ke snížení nákladů o přibližně 100 000 Kč, protože, nebudou zakoupeny nejnákladnější položky. Nicméně při použití levnějšího řešení nebude dostatečně zajištěna ochrana sítě. Rovněž bude složitější správa pracovních stanic, stejně tak vynucování zásad pravidel pro hesla bude mnohem složitější a předpokládám, že opět vzrostou rizika v oblasti zálohování a oblasti týkající se bezpečnosti zejména rizik týkajících se připojování cizích zařízení.

2.7 Přínosy provedených opatření

Při používání Office 365 plánu A2 , jehož součásti je OneDrive. Dojde k omezení používaní vyměnitelných paměťových zařízení. S tímto souvisí také riziko úniku citlivých dat.

Součástí plánu je ještě web podnikového intranetu, který by mohl být alternativou pro sdílení směrnic, a webové konference, kde mohou účastníci komunikovat prostřednictvím videa, sdílet obrazovky a zasílat rychlé zprávy. Toto je pro řešení záležitostí, při kterých je nutný přechod některých zaměstnanců a jejich hromadná domluva na jiné pracoviště. Tímto by odpadla doba, která je potřeba pro přesun zaměstnance na jiné pracoviště a zpět.

Vynucováním zásad bezpečnosti pomocí doménového řadiče dojde ke zvýšení zabezpečení. A Tím ke zvýšení bezpečnosti informací a ke snížení rizika úniku citlivých informací, která podléhají Zákonu č. 101/2000 Sb., o ochraně osobních údajů. Kde za správní delikty proti tomuto zákonu hrozí postihy v jednotkách milionů Kč. Aby organizace postih nedostala, musela by prokazovat: § 46 odst. 1 *„Právnická osoba za správní delikt neodpovídá, jestliže prokáže, že vynaložila veškeré úsilí, které bylo možno požadovat, aby porušení právní povinnosti zabránila.“*[44]

Zálohováním, pomocí řadiče domény se souborovým serverem a NAS serverem se zabrání možné ztrátě dat, a tedy nákladům na jejich obnovu. Ke ztrátě dat už jednou došlo, kdy začátkem roku 2008 selhal disk na jednom z pracovišť, kde byly mzdy a účetnictví. Záloha nebyla prováděna vůbec. Takže obnova v tom roce vyšla na částku kolem 19000 Kč. Úspěšnost obnovy dat není stoprocentní. Je možné, že data se zachránit nepodaří. Popřípadě se již také

[44] Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů

stalo, že frekvence záloh byla nedostatečná. V případě, že záloha bude např. měsíc stará a zaměstnanec bude data znovu vkládat, to v podstatě způsobí, že mu organizace zaplatí znovu za to, co už jednou dělal, i když mu to nebude již třeba trvat tak dlouho.

Řadičem domény, pomocí něhož se pro uživatele zakáže možnost instalace aplikací. V případě, že je nainstalována aplikace porušující Zákon č. 121/2000 Sb., (autorský zákon), odpovědnost za instalované programy leží i na organizaci, kde z porušení tohoto zákona hrozí postihy v řádech desítek tisíc korun.[45]

VPN propojení jednotlivých pracovišť umožní přístup k některým zdrojům, jako je možnost sdílení souborů z jednoho místa pro všechna pracoviště, a přístup k tiskárnám a dalším zařízením zapojeným v síti na jednotlivých pracovištích, což přinese zefektivnění výměny dokumentů. Taktéž to umožní vzdálenou pomoc uživatelům, popřípadě možnost práce z domova, zejména v případě, kdy je zaměstnanec hůře nahraditelný. Takto může vykonat část práce z domova, aniž by bylo nutné proškolovat dalšího zaměstnance a toto školení u něj pravidelně opakovat, protože je pravděpodobné, že po třech měsících by práci za jiného zaměstnance nebyl schopen vykonat.

[45] Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon)

3 ZÁVĚR

Cílem diplomové práce bylo analyzovat stávající stav informačního systému vybrané organizace a jeho efektivnost, posoudit tento stav a navrhnout změny směřující ke zlepšení stávajícího stavu a eliminaci nalezených rizik.

První část práce se věnovala teoretickému popisu a definicím týkajícím se informačních systémů, dále byla popsána metoda HOS 8 a metoda Hodnocení efektivnosti informačních systémů na portálu ZEFIS. V teoretické části byl dále zmíněn pojem riziko a informační bezpečnost.

Analýzu organizace jsem provedl pomocí dotazníků z portálu ZEFIS, které vyplnili zaměstnanci organizace a vlastním šetřením v organizaci. Průzkumem bylo zjištěno, že informační systém používaný v organizaci je přiměřený, nicméně byly zjištěny závažné nedostatky týkající se zejména bezpečnosti a organizačních pravidel IS. Z této oblasti také plynula nejzávažnější rizika týkající se bezpečnosti. V analýze rizik jsem se poté snažil, na základě analýzy a průzkumu v organizaci, identifikovat hrozby, které po jejich eliminaci sníží rizika.

K nejzávažnějším hrozbám a tedy rizikům byla navržena vhodná opatření k jejich snížení a též zvážena finanční stránka nutná pro změnu stavu. Podle mého názoru by měla některá opatření nejen snížit rizika, ale měla by mít i pozitivní účinky především pro zefektivnění práce.

Myslím, že cíle, které byly pro tuto práci vytyčeny, byly splněny.

SEZNAM POUŽITÝCH ZDROJŮ

(1) JANÍČEK, Přemysl a Jiří MAREK. *Expertní inženýrství v systémovém pojetí*. 1. vyd. Praha: Grada, 2013, 592 s. ISBN 978-80-247-4127-7.

(2) BÉBR, Richard a Jiří MAREK. *Informační systémy pro podporu manažerské práce*. 1. vyd. Praha: Professional Publishing, 2005, 592 s. Expert (Grada). ISBN 80-864-1979-7.

(3) MOLNÁR, Zdeněk a Jiří MAREK. *Efektivnost informačních systémů*. 1.vyd. Praha: Grada Publishing, 2005, 142 s. Expert (Grada). ISBN 80-716-9410-X.

(4) VYMĚTAL, Dominik a Jiří MAREK. *Informační systémy v podnicích: teorie a praxe projektování*. 1. vyd. Praha: Grada, 2009, 142 s. Expert (Grada). ISBN 978-80-247-3046-2.

(5) BASL, Josef. *Podnikové informační systémy: podnik v informační společnosti.* 2., výrazně přeprac. a rozš. vyd. Praha: Grada, 2008, 283 s. ISBN 978-80-247-2279-5.

(6) ŠMÍD, Vladimír. *Management informačního systému* [online]. [cit. 2014-01-14]. Dostupné z: http://www.fi.muni.cz/~smid/mis-mdis.htm.

(7) KOCH, Miloš a Kol. *Management informačních systémů*. Vyd. 2., přeprac. Brno: Akademické nakladatelství CERM, 2010, 171 s. Učební texty vysokých škol. ISBN 978-80-214-4157-6.

(8) VOŘÍŠEK, Jiří. *Strategické řízení informačního systému a systémová integrace*. Vyd. 1. Praha: Management Press, 2006, 323 s. ISBN 80-859-4340-9.

(9) SODOMKA, Petr. *Informační systémy v podnikové praxi*. Vyd. 1. Brno: Computer Press, 2006, 351 s. ISBN 80-251-1200-4.

(10) STRNÁD, Ondrej. *Systémový prístup k riadeniu informačnej bezpečnosti*. 1. vyd. Trnava (Slovensko): SP Synergia, 2008. 233 s. ISBN 978-80-89291-20-5.

(11) MŠ Boskovice. *Údaje o MŠ* [online]. 2014 [cit. 2014-04-14]. Dostupné z: http://www.msboskovice.cz/o-nas-2

(12) Město Boskovice, Zřizovací listina Příspěvkové organizace města Boskovice Mateřská škola Boskovice, schválená Zastupitelstvem Města Boskovice č. 5.2 ze dne 14. 9. 2009

(13) Město Boskovice Dodatek č.7 ke zřizovací Příspěvkové organizace MŠ Lidická ul. Schválen dne 16. 6. 2008

(14) *Vema – Informace o produktech*. Vema, a. s., [online], 2014 [cit. 16. 04. 2014]. Dostupné z: http://www.vema.cz/default.aspx?categoryID=Produkty.1

(15) LUŇÁK, Vlastimil. *Uživatelský manuál - Evidence jídelny* L.V-software 2014., 64 s.

(16) KOCH, Miloš. HOS 8. *ZEFIS: Hodnocení informačních systémů* [online]. 2013. [cit. 2014-04-18]. Dostupné z: http://www.zefis.cz/index.php?id=220

(17) KOCH, Miloš. Průzkum efektivnosti IS. *ZEFIS: Hodnocení informačních systémů* [online]. 2013. [cit. 2014-04-18]. Dostupné z: http://zefis.cz/index.php?id=210

(18) SMEJKAL Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 4., aktualiz. a rozš. vyd. Praha: Grada, 2013, 483 s. Expert (Grada). ISBN 978-80-247-4644-9.

(19) Rack skříň. ITEK S.R.O**.** *itek.cz* [online]. 2013. [cit. 2014-04-20]. Dostupné z: http://pc.itek.cz/rackove-skrine-skrine-do-100-cm/X9996621-Rack-GF6942

(20) Server IBM x3650M4 ALZA.CZ A.S. *alza.cz* [online]. 2014. [cit. 2014-04-20]. Dostupné z: http://www.alza.cz/ibm-x3650m4-d1081658.htm

(21) IBM 2.5" HDD 600GB SAS ALZA.CZ A.S. *alza.cz* [online]. 2014. [cit. 2014-04-20]. Dostupné z: http://www.alza.cz/ibm-2-5-hdd-600gb-sas-6g-10000-ot-hot-swap-d1132984.htm

(22) APC Smart-UPS C 1000VA ALZA.CZ A.S. *alza.cz* [online]. 2014. [cit. 2014-04-20]. Dostupné z: http://www.alza.cz/apc-smart-ups-c-1000va-2u-rm-lcd-d457073.htm

(23) Synology DiskStation DS214+ NAS ALZA.CZ A.S. *alza.cz* [online]. 2014. [cit. 2014-04-20]. Dostupné z: http://www.alza.cz/synology-diskstation-ds214-d504189.htm

(24) Western Digital Red 2000GB 64MB HDD ALZA.CZ A.S. *alza.cz* [online]. 2014. [cit. 2014-04-20]. Dostupné z: http://www.alza.cz/western-digital-red-2000gb-64mb-cache-d342211.htm

(25) CISCO RV320-K9-G5 Router VPN ALZA.CZ A.S. *alza.cz* [online]. 2014. [cit. 2014-04-20]. Dostupné z: http://www.alza.cz/cisco-rv320-k9-g5-d510250.htm

(26) ESET File Security pro Microsoft Windows Server ESET SOFTWARE SPOL. S R.O. *eset.com* [online]. 2014. [cit. 2014-04-20]. Dostupné z: https://koupit.eset.com/default.aspx?pid=9&__utma=66954481.720946759.1400770574.1400770574.1400770574.1&__utmb=66954481.24.10.1400770574&__utmc=66954481&__utmx=-

(27) Kurzy vyhlašované ČNB. ČESKÁ NÁRODNÍ BANKA., *cnb.cz* [online]. 2014. [cit. 2014-05-22]. Dostupné z: http://www.cnb.cz/cs/index.html

(28) Plány a ceny služeb Office 365 Education MICROSOFT S.R.O., *office.microsoft.com* [online]. 2014. [cit. 2014-04-22]. Dostupné z: http://office.microsoft.com/cs-cz/academic/porovnani-planu-office-365-education-FX103045755.aspx

(29) D&COMM s.r.o. *Ceník SW Microsoft*. Březen 2014

(30) OneDrive system requirements MICROSOFT INC., *windows.microsoft.com* [online]. 2014. [cit. 2014-04-22]. Dostupné z: http://windows.microsoft.com/en-us/onedrive/system-requirements

(31) Sdílení souborů MICROSOFT S.R.O., *office.microsoft.com* [online]. 2014. [cit. 2014-04-22]. Dostupné z: http://office.microsoft.com/cs-cz/business/nastroje-office-365-pro-sdileni-souboru-a-online-spolupraci-FX102997013.aspx

(32) Co je VPN MICROSOFT S.R.O., *technet.microsoft.com* [online]. 2014. [cit. 2014-04-22]. Dostupné z: http://technet.microsoft.com/cs-cz/library/cc731954%28v=ws.10%29.aspx

(33) VPN – vzdálené připojení SCHINDLER SYSTEMS, S.R.O., *schindler-sys.cz* [online]. 2014. [cit. 2014-04-26]. Dostupné z: http://www.schindler-sys.cz/vpn-vzdalene-pripojeni/

(34) Stavíme Doménový řadič a další služby sítě, BCV SOLUTIONS S.R.O., *bcvsolutions.eu* [online]. 2014. [cit. 2014-04-27]. Dostupné z: http://blog.bcvsolutions.eu/stavime-domenovy-radic-a-dalsi-sluzby-site-uvod/

(35) Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů

(36) Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon)

SEZNAM ZKRATEK

IS	Informační systém
IT	Informační technologie
ICT	Informační a komunikační technologie
ERP	Plánování a řízení podnikových zdrojů
HDD	Pevný disk
RAID	Vícenásobné diskové pole
SLA	Smlouva o úrovni poskytovaných služeb
UPS	Nepřerušitelný zdroj napájení
VPN	Virtuální privátní síť
MS	Microsoft
SAS	Sériová sběrnice k připojování pevných disků
RPM	Otáčky za minutu
NAS	Síťově přístupné úložiště
EDU	Vzdělávání
CAL	Klientská přístupová licence
SW	Software
HW	Hardware
PC	Osobní počítač

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM GRAFŮ