VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

ÚSTAV SOUDNÍHO INŽENÝRSTVÍ

INSTITUTE OF FORENSIC ENGINEERING

POSOUZENÍ INFORMAČNÍHO SYSTÉMU U VYBRANÉ FIRMY A NÁVRH ZMĚN

INFORMATION SYSTEM ASSESSMENT AND PROPOSAL FOR ICT MODIFICATION

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Filip Méheš**
AUTHOR

VEDOUCÍ PRÁCE — **doc. Ing. Miloš Koch, CSc.**
SUPERVISOR

BRNO 2016

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
ÚSTAV SOUDNÍHO INŽENÝRSTVÍ

Zadání diplomové práce

Ústav:	Ústav soudního inženýrství
Student:	**Bc. Filip Méheš**
Studijní program:	Rizikové inženýrství
Studijní obor:	Řízení rizik firem a institucí
Vedoucí práce:	**doc. Ing. Miloš Koch, CSc.**
Akademický rok:	2015/16

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 u vybrané firmy a návrh změn

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 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 978-80-2-7-2279-5.

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.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2015/16

V Brně, dne

L. S.

.....

doc. Ing. Aleš Vémola, Ph.D.
ředitel

Abstrakt

Dipomová práca obsahuje vysvetlenie základných pojmov a princípov využívaných v problematike informačných systémov. Súčasťou práce sú analýzy súčasného stavu informačného systému vo vybranej firme a posúdenie jeho efektívnosti. Na základe týchto analýz je navrhnutý súbor riešení na zlepšenie súčasného stavu a elimináciu rizík z hľadiska vyváženosti a efektívnosti informačného systému.

Abstract

The diploma thesis contains a clarification of the fundamental notions and the principles utilized in the informational systems issues. The analysis of the contemporary condition of the information system applied in a particular company and the evaluation of its effectiveness are the essential parts of the thesis. On the basis of these analyzes, a set of solutions is designed to improve present conditions and eliminate the risks, in terms of stability and effectiveness of the information system.

Kľúčové slová

Informačný systém, dáta, analýza, efektívnosť, riziko, Zefis, HOS 8.

Keywords

Information system, data, analysis, efficiency, risk, Zefis, HOS 8.

Bibliografická citácia

MÉHEŠ, F. *Posouzení informačního systému u vybrané firmy a návrh změn*. Brno: Vysoké učení technické v Brně, Ústav soudního inženýrství, 2016. 85 s. Vedúci diplomovej práce doc. Ing. Miloš Koch, CSc..

Čestné prehlásenie

Prehlasujem, že predložená diplomová práca je pôvodná a spracoval som ju samostatne. Prehlasujem, že citácie použitých prameňov sú úplné, že som vo svojej práci neporušil autorské práva v zmysle Zákona č. 121/2000 Sb., o práve autorskom a o právach súvisiacich s právom autorským.

V Brne dňa 27. 5. 2016

……

Poďakovanie

Chcel by som poďakovať pánovi doc. Ing. Milošovi Kochovi, CSc., vedúcemu diplomovej práce, za jeho ústretový prístup, cenné pripomienky, rady a za možnosť využiť k vypracovaniu analýz portál Zefis.

Obsah

Úvod

Informačné a komunikačné technológie sú neustále modernejšie a potrebnejšie, v rámci celej spoločnosti sa stávajú neoddeliteľnou súčasťou života aj pri tých najrutinnejších činnostiach. Z hľadiska aktuálnych trendov v produktoch určených pre podniky je vidieť zameranie na komplexnosť, online služby a mobilný prístup, ktoré sú zamerané na rôzne obory podnikania a ich využitie je tak veľmi rôznorodé. Takmer žiadna firma sa dnes nedá prevádzkovať bez výpočtovej techniky. Nevyhnú sa jej ani malé podniky s niekoľkými zamestnancami. Potreba zdieľať dáta, pripájať sa k internetu alebo tlač dokumentov a, v neposlednom rade, komunikácia s vonkajším svetom vedie k nutnosti informačné systémy využívať. Výber a následná implementácia informačného systému je pomerne zložitý proces, ktorý vyžaduje aby jeho nastavenie, spolu so zvolenou stratégiou, bolo v praxi využívané a pomáhalo v uľahčovaní činnosti a procesov, čo bude predstavovať pre podnik prínos, v opačnom prípade hrozí riziko strát. Informačný systém by mal byť optimálne nastavený tak, aby odpovedal veľkosti, požiadavkám a finančným možnostiam podniku, aby podporoval zamestnancov pri práci, umožňoval získavanie správnych dát v rámci celej firmy a bol schopný jednoducho sa integrovať a prispôsobiť procesom a ostatným systémom.

Prvá časť práce, na základe odbornej literatúry, spracováva v teoretickej rovine problematiku informačných systémov, riadenia ich efektívnosti, takisto aj oblasti informačnej bezpečnosti a zdôraznenie dôležitosti analýz rizika. Prehľad odbornej literatúry poskytuje potrebnú znalosť informačných systémov pre orientáciu v ďalších častiach. V druhom celku sa vybrané analytické metódy využijú na získanie podkladov pre návrhovú časť, ktorá pozostáva z analýzy hrozieb a prezentácie návrhov opatrení na zefektívnenie informačného systému konkrétnej firmy a k minimalizácií nežiaducich rizík.

Diplomová práca má pomôcť ako východisko pre rozhodnutie managementu v oblasti riadenia informačného systému a prístupom k riešeniu situácie so slabými miestami a nedostatkami.

Cieľ diplomovej práce

Analyzovať súčasný stav informačného systému vybraného podniku a jeho efektívnosti, tento stav zhodnotiť a navrhnúť zmeny, smerujúce k zlepšeniu súčasného stavu a odstráneniu nájdených rizík.

1. TEORETICKÉ VÝCHODISKA PRÁCE

1.1 Základné pojmy

Dáta

Dáta predstavujú údaje, ktoré sa používajú pre popis určitého javu, alebo pre vlastnosť objektu, ktorý pozorujeme (Škrivánek, 2004, online).

Informácia

„Informáciou rozumieme dáta, ktorým ich užívateľ prisudzuje určitý význam a ktoré uspokojujú konkrétnu informačnú potrebu svojho príjemcu. Nositeľom informácie sú číselné dáta, text, zvuk, obraz, prípadne ďalšie zmyslové vnemy. Na rozdiel od dát (zvukov, obrázkov apod.) nemôžeme informáciu skladovať. Na druhej strane informácie ako zdroj poznania sú zdrojom obnoviteľným, nevyčerpateľným.“ (Molnár, 2001, s. 15)

Odborná literatúra, už tradične ponúka mnoho odlišných pojmov definície informácia. Rozdiely sú znateľné hlavne v kladení rôzneho dôrazu na spôsob nahliadania na informáciu. Sodomka (2010, s. 20) píše o nahliadaní z hľadiska modernej podnikovej informatiky:

- Syntaktický pohľad – je orientovaný na vnútornú štruktúru a súvislosti medzi znakmi informácie, bez ohľadu na vzťah voči prijímateľovi.
- Sémantický pohľad – zdôrazňuje obsah a význam informácie, rovnako bez ohľadu na vzťah k príjemcovi.
- Pragmatický pohľad – smeruje k praktickému využitiu informácie, tak aby mala pre príjemcu nejaký význam. Tento pohľad je najbližší managementu a ľuďom, ktorý informácie chápu ako nevyhnutnú časť svojej práce.

Znalosti

Vyplývajú zo schopnosti učiť sa, porozumeniu informácie, ktorá bola práve obdržaná a jej integrácie so skoršími informáciami. Znalosti je možné opísať, ako informácie o tom, ako využiť iné informácie a dáta v rôznych životných situáciách (Šlapák, 2003, online).

Informačné technológie

Sú nástroje, metódy a znalosti, vďaka ktorým je možné spracovávať dáta, z ktorých sa následne tvoria informácie. Týmto termínom možno označiť všetky technológie využité na skladanie informačných systémov. Vzťahu medzi informačným systémom a informačnými technológiami sa dá rozumieť tak, že informačný systém reprezentuje potrebu nejakých informácií, pričom pokrytie tejto potreby predstavujú informačné technológie (Molnár, 2001, s. 12). Informačnými technológiami sa rozumie hardware a software.

Proces

Proces je možné pokladať za organizovanú skupinu činností alebo sub-procesov, ktoré spolu vzájomne súvisia, prechádzajú jedným alebo viacerými organizačnými útvarmi, ktoré spotrebovávajú materiálne, ľudské, finančné a informačné vstupy a ich výstupom je produkt s hodnotou pre konkrétneho zákazníka (Šmída, 2007, s. 29).

1.2 Informačný systém

Molnár (2001, s. 15) rozumie systém v pojatí systémov ako usporiadanú množinu prvkov vrátane ich vlastností a vzájomných vzťahov, ktoré ako celok vykazujú konkrétne vlastnosti. Zjednodušene povedané systém je množina vzájomne prepojených komponentov, ktoré, aby určitý systém naplnil svoj cieľ, musia pracovať spoločne v rámci celého systému ako celok.

Definícií informačného systému existuje mnoho a každá ho vystihuje rôzne, v kontexte tejto práce bude chápaný ako:

„Informačný systém je možné definovať ako súbor ľudí, metód a technických prostriedkov zaisťujúcich zber, prenos, uchovanie, spracovanie a prezentáciu dát s cieľom tvorby a poskytovania informácií podľa potrieb príjemcov informácií činných v systémoch riadenia“(Tvrdíková, 2000 s. 10).

„Informačný systém je komplex informácií, ľudí, použitých informačných technológií, organizácie práce, riadenia chodu systému (zabezpečuje prepojenie na prostredie) a konečne technických prostriedkov a metód slúžiacich k zberu, prenosu, uchovaniu a

ďalšiemu spracovaniu dát za účelom tvorby a prezentácie informácií“ (Rábová, 2008, s. 8).

Uvedené definície majú spoločné, že sa zhodujú v tom, že informačný systém je ucelenou formou využitia informačných technológií v sociálne-ekonomických systémoch. V praxi to znamená, že informačný systém sa skladá z nasledujúcich komponentov (Tvrdíková, 2000 s. 10):

- HW (technické prostriedky) - predstavujú počítačové systémy rôzneho druhu a veľkosti, ktoré sú doplnené o potrebné periférne jednotky, ktoré sú v prípade potreby prepojené prostredníctvom počítačových sietí a napojené na diskový subsystém pre prácu s veľkými objemom dát.

- SW (programové prostriedky) – sú tvorené systémovými programami riadiacimi chod počítača, efektívnou prácou s dátami a komunikáciou počítačového systému so skutočným svetom a programami aplikačnými, ktoré riešia určité triedy úloh určitých tried užívateľov.

- Orgware (organizačné prostriedky) – tvorené súborom nariadení a pravidiel definujúcich prevádzku a využívanie informačného systému a informačných technológií.

- Peopleware (ľudská zložka) – rieši otázky adaptácie a účinného fungovania človeka v počítačovom prostredí do ktorého bol zaradený,

- Reálny svet – berie do úvahy legislatívu, normy a informačné zdroje v kontexte informačného systému.

Ak má informačný systém firmy či inštitúcie byť efektívny, nesmie byť pri vývoji a implementácii zanedbaná žiadna z týchto položiek (Tvrdíková, 2000, s. 10).

1.3 Podnikové informačné systémy

1.3.1 Životný cyklus informačného systému

- 1. fáza – Plánovanie, rozhodnutie, analýza – je dôležité, aby sa manažment spoločnosti v tejto fáze rozhodol, či je potreba nového informačného systému, alebo len jeho inovácie. V rámci tejto fázy by sa mali obsiahnuť požiadavky

na budúci systém, charakteristiku jeho cieľov, prínosov a analýz dopadu tohto rozhodnutia na úroveň podnikania a organizácie. Odpovedať na otázky čo potrebujeme, ako to získame, k čomu nám to bude a aký to prinesie úžitok.

- 2. fáza – Obstaranie, výstavba a voľba implementačného partnera – podnik sa rozhodne akou formou produkt obstará - buď ho sám vyvinie, nechá vyvinúť externou spoločnosťou, alebo sa zakúpi komplexný IS od dodávateľov, alebo prenájmom IS od dodávateľov (outsorcing). Dôležitými metrikami by nemala byť len cena, ale aj funkcionalita, údržba, referencie.
- 3. fáza – uzavretie zmluvného vzťahu – jedna z najpodceňovanejších a zároveň najkritickejších fáz celého cyklu. Zmluvy, so špecifickou terminológiou, ktorá nemusí byť obsiahnutá ani v zákonoch.
- 4. fáza – Zavádzanie, implementácia – obstaraný informačný systém sa zavádza do reálnej prevádzky. Prispôsobuje sa a nastavujú sa parametre, tak aby čo najviac vyhovoval podniku. Často sa v tejto fáze vykonávajú procesné, organizačné aj personálne zmeny.
- 5. fáza – Užívanie, údržba – praktická prevádzka v bežnom podnikovom režime. Odstraňujú sa zistené nedostatky, vylepšuje sa systém, prípadne implementujú nové vzniknuté požiadavky a to nielen na začiatku, ale počas celej doby využívania systému, tak aby bola umožnená realizácia jeho prínosu. Každý výpadok môže mať kritický dopad na podnik, preto je nevyhnutná zazmluvnená správa a údržba.
- 6. Fáza – Rozvoj, inovácia, likvidácia – v rámci tejto etapy sú integrované do podnikového systému ďalšie aplikácie, ktoré detailnejšie pokrývajú kľúčové procesy za účelom získania dodatočných prínosov. Zmeny môžu byť vykonané aj v prípade neaktuálnosti systému, ktorý už nespĺňa nároky. V momente prílišnej zastaranosti ide systém do likvidácie. Tým sa ukončí etapa životného cyklu daného systému (Sodomka 2010, s. 96).

1.3.2 Rozdelenie podľa architektúr

Globálna architektúra je základnou schémou, ideou IS. Tvoria ju stavebné bloky, ktoré vyjadrujú hrubú podobu budúceho informačného systému (Koch, 2004, s. 5).

Globálna architektúra sa ďalej člení a špecifikuje na **čiastkové architektúry:**

Funkčná architektúra – postupe dekomponuje globálnu architektúru a tým rozdeľuje IS na subsystémy až k elementárnym funkciám.

Procesná architektúra – je zameraná na popis neautomatizovaných činností a funkcií IS a ich reakcií na udalosti, ku ktorým môže dôjsť. Jej cieľom je čo najefektívnejšia reakcia podniku na externé udalosti.

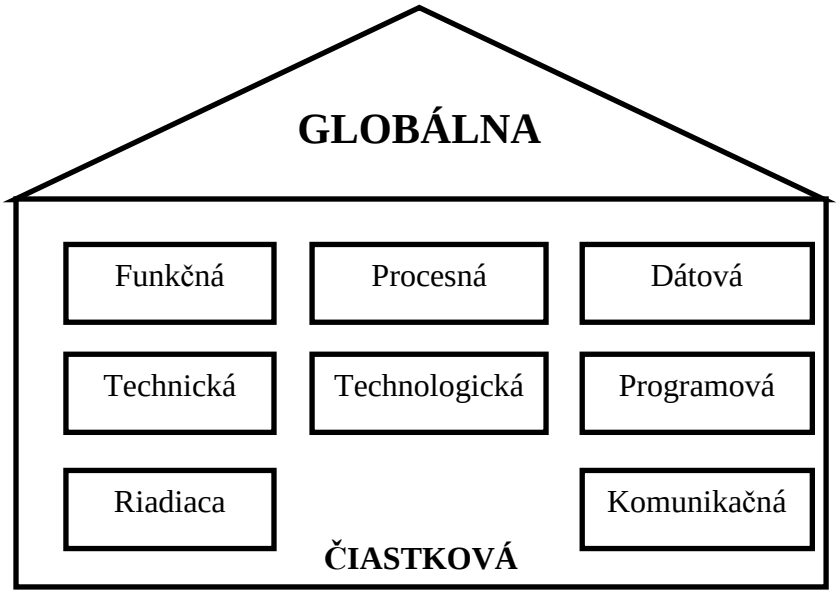
Technická (hardwarová) architektúra – určuje rozmiestnenia prostriedkov výpočtovej a komunikačnej techniky a jej typy. Znázornená býva schémou a špecifikáciou počítačových sietí, serverov, počtom koncových užívateľských počítačov a ďalších zariadení.

Technologická architektúra – určuje spôsob spracovania aplikácií, ktoré nadväzujú na technickú, dátovú a programovú architektúru. Jedná sa o spôsob spracovania aplikácií a dát, vnútornú stavbu aplikácií a užívateľské rozhranie aplikácie.

Dátová architektúra – predstavuje návrh dátovej základne organizácie. Pri návrhu vychádzame z definície jednotlivých objektov a ich položiek a väzbami medzi nimi. Výsledkom dátovej architektúry je schéma všetkých databáz.

Programová (softwerová) architektúra – určuje, z ktorých programov a programových komponentov sa bude vo výsledku skladať informačný systém a aké väzby medzi nimi budú.

Komunikačná a riadiaca architektúra – externé rozhranie systému a komunikácie s okolím, definícia pravidiel fungovania systému a orgware (Koch, Ondrák, 2004, s. 5).



Obrázok 1: IS z pohľadu architektúr
(Zdroj: Vlastné spracovanie podľa Koch a kol., 2010, s. 14)

1.3.3 Rozdelenie podľa úrovne riadenia

V podniku sa zvyčajne rozoznávajú tri riadiace vrstvy. Úroveň riadenia strategická, taktická a operatívna. Kým podľa riadiacej pyramídy najnižšia, operatívna úroveň riadenia, potrebuje najväčšie množstvo informácií, najvyššia, strategická úroveň využíva veľké množstvo informácií, predovšetkým z okolia podniku a vysoko agregované informácie z vnútra podniku (Koch, 2010. s. 15).

CIM (Compurwe Integrated MAnufacturing) – počítačom integrovaná výroba zahŕňajúca riadenie technologických procesov. Medzi tieto sa je počítajú NC stroje, ktoré sú riadené počítačom. Je to predchodca ERP.

ERP (Enterprise Resouorce Planning) – nástupcovia CIM. Pokrývajú celkovú problematiku podnikových procesov – plánovanie, riadenie zdrojov, financie.

TPS (Transaction proccessing Systems) – nástupcovia klasických dávkových systémov, ktoré sa nachádzajú u pracovníka. Ide napríklad o agendu objednávky tovarov. Používajú sa najmä pri operatívnom riadení.

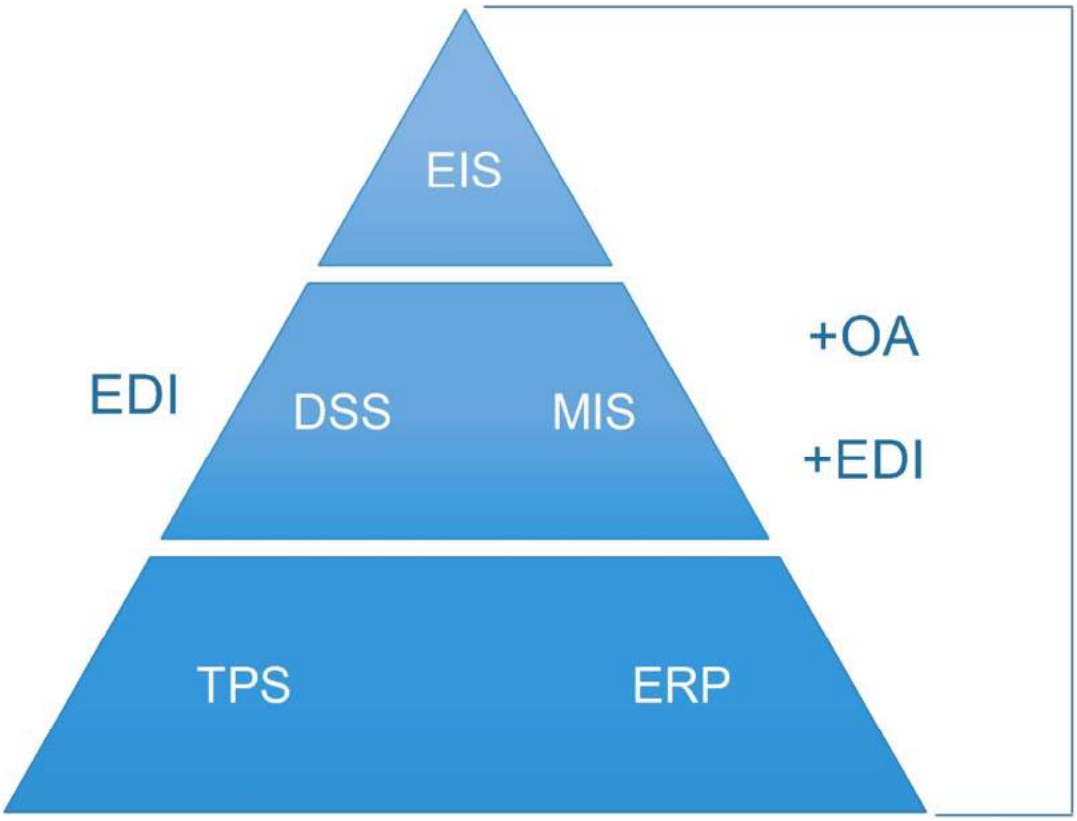
MIS (Management Information Systems) – ich korene je možné vidieť v ekonomických a účtovných systémoch. Tieto systémy sú určené pre taktické riadenie, Ich hlavnou činnosťou je sumarizácia a agregácia dát za určité obdobie.

DSS (Decision Support Systems) – systémy určené pre podporu rozhodovania. Najčastejšie sa analyzujú dáta z MIS, ktoré sú určené pre taktické a strategické riadenie. Jedná sa o jednorazové úlohy s grafickými výstupmi.

OA (Office Administration) – prípadne automatizácia administratív, ktorá využíva textové editory, elektronický kalendár, elektronickú poštu na všetkých úrovniach riadenia.

EIS (Executive Information Systems) – sú systémy pre vrcholové vedenie. Umožňujú prístup k externým dátam a podnikové informácie agregujú do najvyššej úrovne.

EDI (Electronic Data Interchange) – časť IS na podporu výmeny dát a komunikácie s okolím ako sú zákazníci prípadne banky. (Koch, 2010. s. 15).



Obrázok 2: IS z pohľadu architektúr
(Zdroj: Vlastné spracovanie podľa Koch a kol., 2010, s. 14)

1.3.4 Technologický model IS

Tento pohľad je možné znázorniť pomocou na seba nadväzujúcich vrstiev. Skladá sa z hardwaru, ktorý tvorí základ, na ktorý je naviazaný operačný systém. Pri výbere hardweru je dôležité zmysluplne vyberať komponenty tak, aby bol schopný obsluhovať ďalšie časti, tiež je potrebné brať v úvahu rýchle starnutie. Operačný systém je zvolený s ohľadom na výber ďalších komponentov. Na štandardnom systéme (hardware a software) beží databázový systém, ktorý zaisťuje dátovú podporu pre aplikačný software, ktorý završuje tento pohľad. Existujú aj aplikácie, ktoré nie sú viazané operačným systémom (Basl, Blažíček, 2012, s.101).

Obrázok 3: Technologický model IS
(Zdroj: Vlastné spracovanie podľa Basl, Blažíček, 2012, s.101)

1.3.5 Rozdelenie podľa holisticko-procesného pohľadu

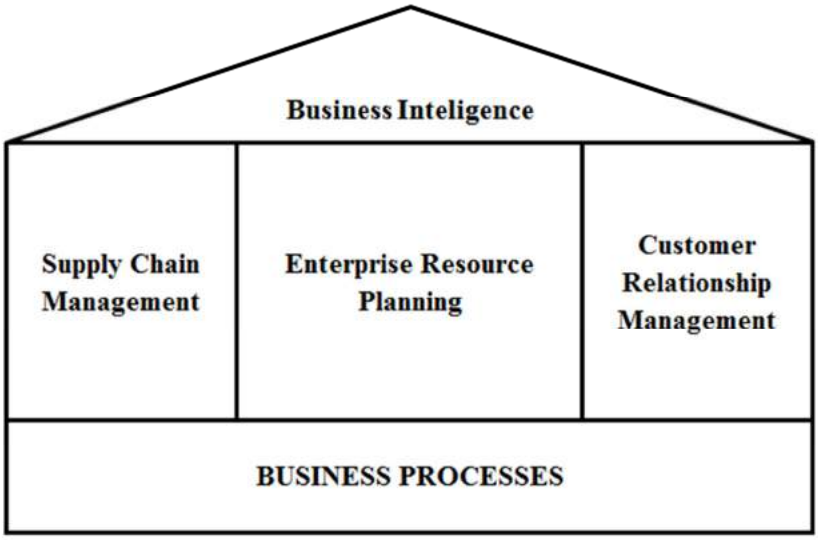
Holistický pohľad na informačný systém je oveľa širší než obvyklý. IS je chápaný ako komplex, ktorý je vytváraný neformalizovanými informáciami (informácie a znalosti ľudí v hlavách), formalizovanými informáciami (informácie zaznamenané, ale nie automatizované) a IS/IT, časť, ktorá je spracovaná pomocou informačných technológií, teda tým, čo si väčšina ľudí predstaví pod pojmom informačný systém. Cieľom je prevádzať neformalizované informácie na formalizované, a tie následne do podoby spracovateľnej pomocou IS/IT (Koch, 2004, s. 8-9). Podľa holisticko-procesnej klasifikácie je informačný systém zložený z:

1) ERP – (Enterprise Resurcing Planning) hlavná časť zameraná na riadenie interných podnikových procesov.

2) CRM – (Costumer Relationship management) je zameraný na riadenie procesov týkajúcich sa zákazníkov.

3) SCM – (Supply Chain Management) riadi procesy zamerané na dodávateľov. Väčšinou je jeho súčasťou APS (pokročilé plánovanie a rozvrhovanie výroby).

4) BI – (Business Intelligence) tiež manažérsky informačný systém, zbiera dáta z ERP, CRM a SCM systémov a na ich základe poskytuje informácie podnikovému managementu pre rozhodovanie (Sodomka, 2010, s. 77).



1

Obrázok 4: Holisticko-procesný pohľad na IS
(Zdroj: Vlastné spracovanie podľa Sodomka, 2010, s. 78)

1.3.6 ERP

Medzi odborníkmi nie je všeobecná zhoda na definícii systémov ERP, respektíve ani na zaradzovaní produktov, ktoré do ERP patria a ktoré nie. Sodomka (2010, s.148) pod systémom kategórie ERP rozumie: *„účinný nástroj, ktorý je schopný pokryť plánovanie a riadenie hlavných interných podnikových procesov (zdrojov a ich transformácie na výstupy), a to na všetkých úrovniach, od operatívnej až po strategickú.“*

K hlavným procesom patria tie, nad ktorým má management plnú kontrolu a patria sem výroba, logistika, ľudské zdroje a ekonomika. Za základné vlastnosti ERP systémov sa posudzujú:

- Automatizácia a integrácia hlavných podnikových procesov
- Zdieľanie dát, postupov a ich štandardizácia skrz celý podnik
- Vytváranie a sprístupňovanie informácií v reálnom čase
- Schopnosť spracovávať historické dáta
- Celostný prístup k presadzovaniu ERP koncepcie

ERP systémy sa delia podľa oborového a funkčného zaradenia a podľa schopnosti pokryť všetky štyri interné procesy (výroba, logistika, personalistika, ekonomika). Rozlišujú sa 3 typy ERP systémov:

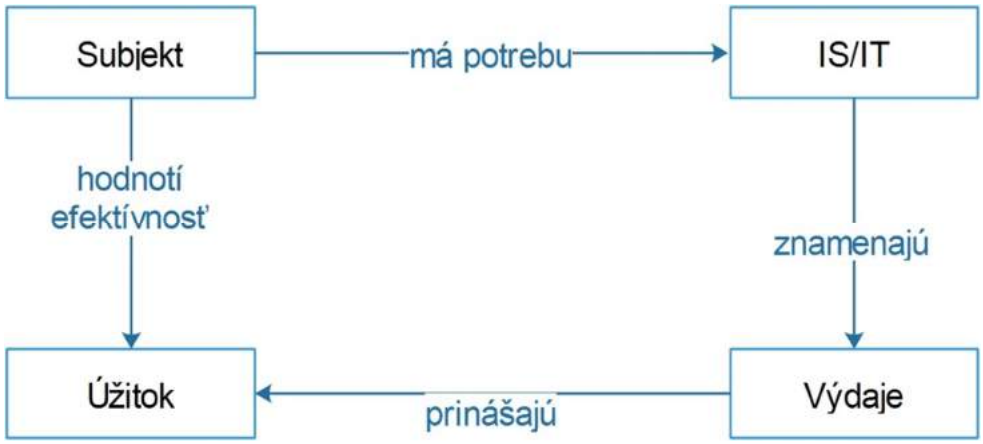
- All-in-One - pokrýva všetky podnikové procesy, t.j. výrobu, personalistiku, logistiku a ekonomiku. Medzi jeho výhody patrí vysoká úroveň integrácie. Nevýhody sú najmä nižšia detailnosť a nákladné prispôsobenia systému podniku.
- Best-of-Breed - orientácia na určité obory podnikania alebo špecifické procesy. Nemusí pokrývať všetky kľúčové procesy. V rámci podniku môže fungovať spoločne s inými OS. Výhodou je detailnejšia funkcionalita a nevýhodou môže byť obťažnejšie sledovanie a riadenie procesov a nutnosť riešiť viacero IT projektov.
- Lite ERP - okliešťená verzia štandardného ERP systému. Je zameraná primárne na malé a stredne veľké podniky, ktoré si nemôžu dovoliť financovať štandardný ERP systém. Výhodou je v tomto prípade nižšia cena a krátka implementácia do podniku. Nevýhodou je menšia dostupnosť funkcií resp. ich obmedzenia, počtu užívateľov prípadne rozšírení.

Skúsenosť v podnikoch postupne začala prinášať požiadavky na tesnejšie prepojenie interných a externých procesov (oblasť riadenia vzťahov medzi zákazníkmi a riadenia dodávateľského reťazca). Pri týchto procesoch nie je presne definovaný vlastník a management v podniku nemá ich riadenie priamo pod kontrolou. ERP systémy sa preto rozvinuli do podoby označovanej ako ERP II, niekedy označované ako rozšírené ERP (extended ERP) (Sodomka, 2010, s. 150-151).

1.4 Riadenie IS

1.4.1 Efektívnosť IS/IT

Úžitok súvisí s efektívnosťou IS – s potrebou informácií vzniká požiadavka na určitý informačný systém. Z uspokojenia tejto potreby je nejaký úžitok. Potrebu IS uspokojí určitá aplikácia IT, ktorá prináša do podniku náklady. Pokiaľ je potreba uspokojenia informáciou vysoká, je vysoký aj úžitok. Dá sa tak predpokladať, že aj efektívnosť vynaložených prostriedkov bude vysoká. Úžitok (utility) je uspokojenie nejakej potreby – musí mať pre subjekt daný význam. (Molnár, 2001, s. 16).



Obrázok 5: Model úžitku IS/IT
(Zdroj: Vlastné spracovanie podľa Molnár, 2001, s. 16)

Hodnotenie efektivity IS/IT nie je len otázkou uspokojenia požiadaviek a potrieb, ale jedná sa predovšetkým o to, kto a aký úžitok očakáva. V rámci podnikovej sféry nájdeme nasledujúce kategórie subjektov a ich očakávania (Molnár, 2001, s. 17):

- Majitelia – očakávajú trvalé zhodnotenie majetku vloženého do podniku.
- Manažéri – očakávajú možnosť efektívneho riadenia, teda dosiahnuť daných výsledkov s minimom prostriedkov vynaložených na správu.
- Zamestnanci – očakávajú lepšie pracovné prostredie, stotožnenie sa s podnikom.
- Zákazníci – by mali dostať tovar s vyššou pridanou hodnotou za prijateľnú cenu.

Každý subjekt hľadá ideálny pomer medzi úžitkom IS/IT a výdavkami potrebnými vynaložiť na získanie úžitku, časom potrebným na získanie úžitku a rizikami spojenými s tým, že sa nedostaví očakávaný úžitok. Ak je systém takto vyvážený, považuje sa za efektívny (Molnár, 2001, s. 17). *„Celá rada výskumov Mahmoos and Maann (1993) Shaw (1994), Berndt and Morrison (1995) Brynjolfsson and Young (1996) ukázala, že investície do IS/IT neprinášajú očakávané efekty v zmysle ekonomickej návratnosti, (napr., že jeden investovaný USD do IS/IT prinesie iba 0,8 USD). Tieto zistenia viedli zmienených autorov k tomu, čo nazývajú paradoxom informačných technológii alebo tiež paradoxom efektivity. Bola nastolená otázka: „Prečo produktivita práce nerastie súčasne s používaním pokrokových IT?“. Brynjolfsoon má pre tento paradox nasledujúce vysvetlenia:*

- *Používanie nesprávnych resp. nevhodných závislostí výstupov na vstupoch.*
- *Veľkým časovým odstupom medzi vstupom (investíciou) do IS/IT a výstupom (prínosom).*
- *Pôsobením faktoru redistribúcie prínosov, ktorý sa uplatňuje tak, že konkurenčná výhoda, ktorú získa niektorý podnik v dôsledku pionierskej aplikácie IS/IT je rýchlo absorbovaná ostatnými podnikmi.*
- *Zlým riadením investícií do IS/IT spôsobujúcim zbytočné investície resp. ktoré sú stratové“* (Molnár, 2001, s. 18).

Skúmanie problematiky efektívnosti IS/IT je možné založiť na všeobecnom systémovom modely transformácie vstupov na výstupy pri pôsobení transformačných faktorov – vnútorných a vonkajších, ktoré ovplyvňujú efektívnosť transformácie. Koncepcia modelu je zobrazená na nasledujúcom obrázku (Molnár, 2001, s. 18).

Obrázok 6: Koncepčná schéma modelu efektívnosti
(Zdroj: Vlastné spracovanie podľa Molnár, 2001, s. 18)

Na model je možné nazerať z rôznych pohľadov. Najčastejšie sa na tomto modely hľadá odpoveď na otázku: „Ako riadiť rozvoj IS/IT, aby sme s danými obmedzenými výdajmi dosahovali čo najvyšších prínosov pre podnik?“. Ako ďalšia otázka môže slúžiť: „Aké majú byť vstupy, aby sme dosiahli požadovaných prínosov?“. Odpovede je potrebné hľadať ako na strane vstupov, ktoré by pre najväčšiu efektívnosť mali byť minimalizované, tak na strane výstupov, ktoré by mali byť maximalizované.

Rozhodujúce je nachádzanie hodnôt parametrov, ktoré ovplyvňujú túto transformáciu (Molnár, 2001, s. 18).

1.4.2 Informačná stratégia

Stratégia úzko súvisí s firemnými cieľmi, ktoré predstavujú budúce stavy, ktoré sa firma vďaka stratégii snaží dosiahnuť. Informačná stratégia by mala obsahovať víziu, ciele a hlavné charakteristiky budúceho stavu IS/IT firmy a mala by tiež prispievať k zmierňovaniu chaotického riadenia ich vývoja a prevádzky vrátane investícií s tým spojenými. Informačná stratégia má dopomôcť podniku k zvyšovaniu produktivity pracovníkov, podporovaní strategických cieľov firmy a prispievaniu k ďalšiemu rozvoju podniku (Koch, Ondrák, 2004, s. 131).

„Informačnou stratégiou všeobecne rozumieme ako sústavu cieľov a spôsobov ich dosiahnutia. Cieľom informačnej stratégie podniku by malo byť predovšetkým hľadanie odpovedí na otázky ako pomôcť IS/IT:

- *zvyšovať výkonnosť pracovníkov podniku,*
- *podporovať dosahovanie strategických cieľov podniku,*
- *získavať pre podnik konkurenčnú výhodu*
- *vytvárať pre podnik ďalšie strategické príležitosti rozvoja“* (Molnár, 2001 s. 21).

Definovanie informačnej stratégie je výsledkom trvalého dialógu medzi managementom podniku a odborníkmi IT, mal by byť orientovaný na analýzu procesov a možnosť ich podpory IS/IT spolu so systematickou snahou vytvárať potrebnú informačnú štruktúru. Úroveň infraštruktúry je výsledná v závislosti od vyrovnanosti a zodpovedajúcej kvality jej komponentov (hardware, software, dataware, peopleware a orgware) (Molnár, 2001, s. 21).

1.4.3 Informačná bezpečnosť

Informačná bezpečnosť zahŕňa ochranu všetkých informácií bez rozdielu nosiča po celý ich životný cyklus. V súčasnosti sa spája predovšetkým s informáciami, ktoré prechádzajú skrz informačné technológie. V mnohých prípadoch sa jedná o informácie so nezanedbateľnou hodnotou (zdravotné záznamy, bankové účty, platobné nástroje, výsledky vývoja alebo výskumu) - musia byť chránené tak aby k nim mali prístup práve oprávnené osoby, aby bolo dohľadateľné, kto informáciu vytvoril, zmenil, alebo

odstránil, aby ich nebolo možno nekontrolovateľne vyzradiť, aby boli dostupné v momente potreby. Zraniteľnosť informačných systémov sa považuje za ich všeobecnú vlastnosť (Čandík, 2010, online). Bezpečnosť informačného systému je jednou z kľúčových oblastí, ktorej je treba venovať zvýšenú pozornosť. Zničená technika sa dá vždy do určitej miery nahradiť, programy preinštalovať, ale v prípade zničenia, prípadne zneužitia dát, môže podnik čeliť katastrofe. V prípade pohľadu na informačný systém ako čiernu schránku, ktorá je obklopená ochrannými prvkami, ktoré pomáhajú pred vonkajším útokom (počítačové vírusy, zahltenie serverov, fyzické poškodenie, krádež a iné), sa musí vnímať ešte jedno veľmi závažné riziko, a to riziko útoku z vnútra organizácie. Štatistiky potvrdzujú, že najväčšie percento zneužitia dát pochádza práve od zamestnancov daného podniku (Koch, 2010, s. 148). Pre zaistenie trvale dobrého mena podniku a dôveryhodnosti jeho informačného systému je potrebné, pri stálom monitorovaní všetkých funkcií, ktoré zaisťujú bezpečnosť a spoľahlivosť, venovať pozornosť aj personálnemu obsadeniu jednotlivých funkcií, vyhodnocovať riziká a snažiť sa ich odstrániť, alebo aspoň znížiť, prípadne akceptovať ak sú prijateľné (Čandík, 2010). Toto však nie je len izolovaný problém bezpečnosti informačného systému, ale bezpečnosti celej organizácie, preto je potreba vykonať celkovú analýzu rizík (Koch, 2010, s. 148).

Podľa Bébra a Doucka (2005, s. 137) rozlišujeme tri hlavné spôsoby ochrany informačného systému:

- Proti strate alebo zničeniu – rieši otázky prístupnosti informácií. Mal by byť prítomný u všetkých IS. Dáta je potrebné chrániť pred neúmyselným ohrozením ako napríklad pád systému, úmyselným ako vírus, alebo živelnými pohromami.
- Proti zneužitiu – rieši otázky z pohľadu dôveryhodnosti všetkých informácií Pojednáva o prístupoch k jednotlivým súborom, položkám, dokumentom tzv. pasívny prístup.
- Proti nežiaducim zmenám – rieši otázku integrity všetkých druhov informácií. Pojednáva o zadefinovaní právomoci pri aktívnom prístupe ako sú vkladanie alebo úprava dát.

1.5 Riziko

Odborná literatúra definuje pojem riziko rôzne. Definícia rizika záleží na odvetví, obore a problematike. Tým pádom existujú skupiny definícií technických, ekonomických a sociálnych (Milík, Tichý 2006, s. 98). V súčasnosti je možné riziko všeobecne chápať ako nebezpečenstvo vzniku škody, poškodenia, straty alebo zničenia, prípadne nezdaru v podnikaní. Dnešné projektové riadenie poníma riziko ako neistotu či negatívnu udalosť (Veber, 2004, s. 15).

„Riziko je pravdepodobnosť vzniku neštandardného stavu konkrétnej entity v danom čase a priestore“ (Janíček, Marek a kol. 2013, s. 306).

„Riziko je pravdepodobná hodnota straty vzniknutej nositeľovi, poprípade príjemcovi rizika realizáciou scenára nebezpečia, vyjadrená v peniazoch alebo iných jednotkách“ (Milík, Tichý, 2006 s. 40).

Riešením rizík a kríz s nimi spojeným sa zaoberá risk management, teda proces riadenia rizík, kedy sa subjekt snaží obmedziť pôsobenie súčasných aj budúcich rizík a navrhuje sadu navzájom previazaných činností, ktorých cieľom je riadiť potenciál rizika a pomáha k eliminovaniu nežiadaných dopadov. Súčasťou riadenia rizika je rozhodovací proces, vychádzajúci z dôslednej analýzy rizík. Pomocou analýz sa vhodnými opatreniami zníži pravdepodobnosť rizika a závažnosť možných následkov. Veličiny, s ktorými sa pracuje pri analýze rizík je možné vyjadriť niekoľkými spôsobmi. Existujú dva základné prístupy ich vyjadrenia, sú to kvantitatívny prístup a kvalitatívny. Používa sa vždy jeden z nich, alebo ich kombinácia (Smejkal, Rais, 2013 s 108,109):

Kvalitatívne metódy – založené na opise pravdepodobnosti a závažnosti potenciálneho dopadu, riziká sú vyjadrené v rozsahu na bodovej stupnici, alebo určené pravdepodobnosťou alebo slovným spojením. Kvalitatívne metódy sú jednoduché, rýchle a subjektívne.

Kvantitatívne metódy – založené na matematickom výpočte rizika z frekvencie výskytu a jeho dopade, používajú číselné ocenenie, sú náročné na spracovanie, sú však exaktnejšie ako kvalitatívne.

Kombinované metódy – založené na číselných údajoch. Cieľom je snaha viac sa priblížiť realite pomocou kvalitatívneho hodnotenia. Údaje však nemusia vždy presne popisovať pravdepodobnosť kvôli možnému skresleniu použitej stupnice.

Všeobecný postup analýzy rizík predstavuje proces definovania hrozieb, pravdepodobnosti ich výskytu a závažnosti dopadu. Analýzu rizík zahŕňa (Smejkal, Rais, s. 95, 96):

- Identifikácia aktív – vymedzenie daného subjektu a popis jeho aktív, ktoré vlastní; z hľadiska podniku sa jedná o to, čo sa bude posudzovať.
- Stanovenie hodnoty aktív – určenie hodnoty vymedzených aktív, ich významu pre subjekt a vyhodnotenie možného dopadu ich straty, zmeny, či poškodenia na fungovanie prípadne existenciu subjektu.
- Identifikácia hrozieb a slabín – vymedzenie druhov udalostí a akcií, ktoré môžu negatívne ovplyvniť hodnotu aktív, určenie slabých miest subjektu, ktorá môžu umožniť pôsobenie hrozieb.
- Stanovenie závažnosti hrozieb a miery zraniteľnosti – určenie pravdepodobnosti výskytu hrozby a miery zraniteľnosti subjektu voči hrozbe.
- Posúdenie dopadov – v prípade, že dôjde k realizácii hrozby na konkrétne aktívum.
- Stanovenie úrovne rizika.
- Rozhodnutie – či sú rizika akceptovateľné alebo nie, podľa ich úrovne. Pokiaľ sú neakceptovateľné, je potrebné realizovať vhodné opatrenia.

1.6 Hodnotenie IS spoločnosti

1.6.1 SWOT analýza

Jedná sa o komplexnú metódu vyhodnotenia všetkých relevantných stránok fungovania podniku a jej súčasnej pozície. Predstavuje silný nástroj pre celkovú analýzu vnútorných a vonkajších činiteľov a zahŕňa postupy techník strategickej analýzy. Podstata metódy spočíva v zaradení a ohodnotení jednotlivých faktorov silných a slabých stránok, na jednej strane oproti príležitostiam a nebezpečenstvám na strane druhej. Je tak možné získať nové kvalitatívne informácie, ktoré charakterizujú a hodnotia úroveň ich vzájomného stretu. SWOT je skratka anglických slov Strenghts –

silné stránky, Weaknesses – slabé stránky, Opportunities – príležitosti, Threats – hrozby.

SWOT predstavuje kombináciu dvoch analýz S (strenghts = silné stránky) – W (weaknesses = slabé stránky) a O (opportunities = prileżitosti) – T (threats = hrozby). Analýza SWOT predpokladá, že podnik dosiahne strategického úspechu maximalizáciou svojich predností a príležitostí a minimalizáciou nedostatkov a hrozieb (Dědina, Cejthamr, 2005, s. 42). .

1.6.2 Analýza efektivity IS

Nástroj Zefis *(portál tvorený a vyvíjaný doc. Ing. Milošom Kochom, CSc. V rámci jeho výskumu efektívnosti informačných systémov)* slúži pre online prvotné posúdenie efektívnosti firemných informačných systémov, prostredníctvom dotazníkov. Systém využilo v súčasnosti už cez 2500 českých a slovenských podnikov, aby zistili, či majú ich pracovníci lepší informačný systém, než konkurencia, aká je úroveň bezpečnosti dát v podniku, ako pracovníci informačný systém vnímajú, aká je úroveň podpory atď. Výsledkom nástroja Zefis je nie len posúdenie efektívnosti informačného systému, ale aj porovnanie s ostatným firmami v rámci databázy. Výskum prebieha formou online dotazníka obsahujúceho 59 otázok, na ktoré je možné odpovedať výberom jednej z možností. Po uzavretí dotazníku si je možné, podľa hľadiska ako napríklad odvetvie podniku, veľkosť, profesia respondenta, porovnať výsledky s ostatnými spoločnosťami z databázy, ktoré majú absolvovanú analýzu. Vyhodnotené výsledky sú dostupné okamžite po vyplnení dotazníka. Vyhodnotenie je rozdelené do viacerých oblastí, z ktorých každá sa pozerá na informačný systém iným pohľadom (Zefis.CZ, 2016, online):

Nastavenie parametrov – nastavenie parametrov pre porovnanie s ostatnými podnikmi**.**

Firma – vymedzené základné informácie o firme.

Informačný systém – základné posúdenie a údaje o informačnom systéme.

Zamestnanci - informácie o zamestnancoch a ich porovnanie s ostatnými firmami.

Úroveň podpory – posúdenie technickej a užívateľskej podpory informačného systému.

Úroveň riadenia – skúmanie prítomnosti zodpovednej osoby za informačný systém a povedomia o informačnej podnikovej stratégii.

Efektívnosť IS – posúdenie adekvátnosti vynaložených prostriedkov na výsledok a posúdenie, či je IS efektívne nápomocným pracovníkom.

Bezpečnosť IS a chápanie IS ako služby – skúma úroveň zabezpečenia dát; pochopenie informačného systému ako podporný proces alebo integritná súčasť procesov.

1.6.3 Analýza vyváženosti IS

Metóda HOS 8 bola vyvinutá na Ústave informatiky Podnikateľskej fakulty Vysokého učenia technického v Brne. Cieľom tejto metódy je posúdenie informačného systému ako celku na základe ôsmych kľúčových oblastí. Aby bol systém vyvážený, musia byť všetky jeho oblasti na podobnej úrovni, ich nevyváženosť, respektíve jednej oblasti vedie k neefektívnosti celku. Systém sa dá tak prirovnať k reťazi, ktorá je silná presne, ako jej najslabší článok. Skúmané oblasti sú (Koch, 2010, s. 68):

Hardware (HW) – fyzické vybavenie vo vzťahu k jeho spoľahlivosti, bezpečnosti, použiteľnosti so softvérom.

Software (SW) – programové vybavenie, jeho funkčnosť vo vzťahu k užívateľovi.

Orgware (OW) – prevádzka informačných systémov a doporučených pracovných systémov.

Peopleware (PW) – užívatelia informačných systémov vo vzťahu k rozvoju ich schopností, k ich podpore pri užívaní informačných systémov a vnímaniu ich dôležitosti. Cieľom nie je hodnotiť odborné znalosti.

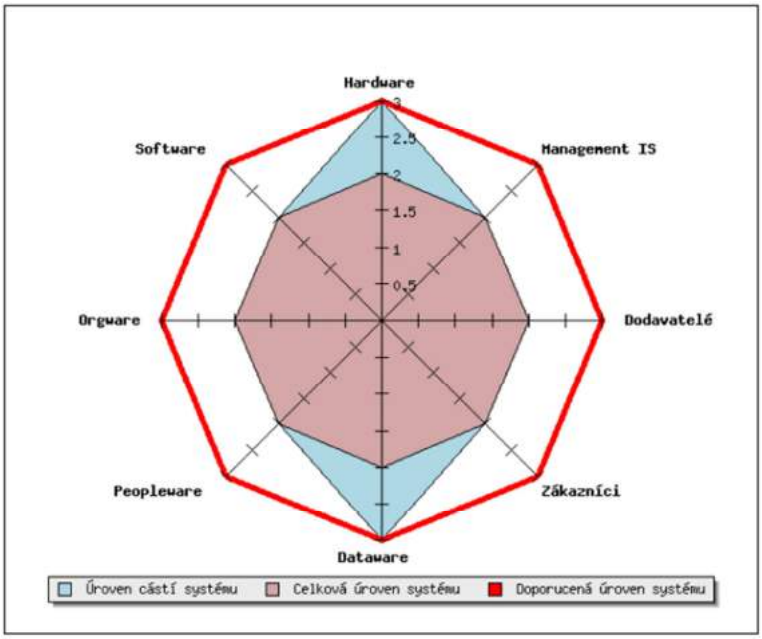
Dataware (DW) – uložené a používané dáta v informačných systémoch, ich dostupnosť, správu a bezpečnosť a spôsob ich využitia užívateľom.

Customers (CU) – aký prínos má informačný systém zákazníkom poskytovať a ako je táto oblasť riadená. Cieľ nie je spokojnosť zákazníka, ale spôsob riadenia oblasti.

Suppliers (SU) – čo informačný systém vyžaduje od dodávateľov a ako je táto oblasť riadená.

Management IS (MA) – riadenie informačného systému vo vzťahu k informačnej stratégii, dôslednosť uplatňovania stanovených pravidiel a vnímanie koncových užívateľov informačného systému. Nízka úroveň tejto oblasti negatívne ovplyvňuje úroveň ostatných, z dôvodu, že riadiaci pracovníci môžu priamo ovplyvňovať ostatné skúmané oblasti.

Každá oblasť je analyzovaná na základe všeobecných otázok, ktoré vyjadrujú vznikajúce problémy v určitej oblasti. Respondent odpovedá formou výberu z niekoľko daných odpovedí, ktoré sú vopred ohodnotené hodnotami (1 = zlá úroveň systému, 3 = vyvážený systém, 4 = veľmi dobrá úroveň systému). Po spracovaní zadaných dát do dotazníku je vyhodnotená úroveň celkového systému, ktorá zodpovedá oblasti s najnižšou úrovňou resp. ohodnotením (Koch, 2010, s. 81).



Obrázok 7: Graf vyváženosti IS metódou HOS8
(Zdroj: Prevziate z portálu Zefis.cz, 2016, online)

Pri aplikácií je potrebné brať do úvahy aj obmedzenia, ktoré metóda má. Metóda HOS 8 neslúži na detailné skúmanie informačných systémov na úrovni jednotlivých procesov. Dosiahnuté výsledky sú založené na subjektívnych odpovediach na kontrolné otázky, ktoré sú všeobecné vzhľadom k relatívne širokému záberu skúmaných informačných systémov (Koch, 2010, s. 83).

Podľa výsledkov zisteného súhrnného stavu, daného významu IS, vyváženosti oblastí a zvolenej stratégie existujú odporúčania vo vzťahu k IS (Koch, 2010, s. 79):

- Stratégia expanzie - predpokladá zacielenie na skokové zlepšenie stavu informačných systémov, spolu so stratégiou vznikajú aj vyššie investície do informačných systémov.
- Stratégia stability – stabilitou sa nemyslí pozastavenie aktivít vo vzťahu k rozvoju a zlepšovaniu efektivity. Cieľom je postupné zvyšovanie efektivity súčasného IS, s čím sú spojené finančné výdaje.
- Stratégia obmedzení – cieľom tejto stratégie je nevkladať do rozvoja a prevádzky informačného systému viacej prostriedkov, než je nutné a získať prostriedky na iné činnosti.

2. ANALÝZA PROBLÉMU A SÚČASNÁ SITUÁCIA

Analytická časť práce má za úlohu predstaviť konkrétnu spoločnosť, vymedziť predmet podnikania, organizačnú štruktúru, vrátane rozboru činností jej zložiek, analyzovať súčasný stav situácie z hľadiska posúdenia informačného systému. V rámci kapitoly je obsiahnuté posúdenie efektívnosti IS, vyhodnotenie metódou HOS 8 a analýza SWOT. Analýzy sú podstatným výstupom kapitoly, ktoré boli získané prostredníctvom vyplnenia dotazníkov v online systéme Zefis, rozhovormi a vlastným pozorovaním.

2.1 Predstavenie spoločnosti

2.1.1 Základné údaje o spoločnosti

Obchodné meno: MARS

Sídlo spoločnosti: Orlové 166, Považská Bystrica 017 01

Dátum zápisu do obchodného registra: 18. Marec 1990

Identifikačné číslo: 10878131

Predmety podnikania:

- sprostredkovanie obchodu
- veľkoobchod v rozsahu voľných živností
- maloobchod v rozsahu voľných živností
- výroba výrobkov z gumy a výrobkov z plastov

2.1.2 Vznik a vývoj spoločnosti

Obchodná spoločnosť MARS vznikla ako spoločnosť s ručením obmedzeným 16. 03. 1990 so zameraním na montáže a rekonštrukcie stavieb. Od roku 1998 sa predmet jej podnikateľskej činnosti rozšíril o veľkoobchod s komplexnou ponukou služieb zákazníkom v oblasti predaja širokého sortimentu výrobkov z technickej gumy, ktoré tvoria nosnú kostru sortimentu ako sú guferá, silentbloky, o-krúžky, manžety, klinové remene, tesniace materiály, náhradné diely do áut, hadice, na ktoré sa nabaľujú všetky ostatné tovary. V priebehu rokov sa sortiment rozšíril aj o vzduchovú a zváraciu techniku s cieľom vybudovať stabilnú spoločnosť na poli týchto trhov, so snahou o postupné získanie silnej pozície na úrovni svojho regiónu. Ako posledné sa do sortimentu zaradili motorové, elektrické zariadenia v podobe hobby alebo profi náradia, či záhradná technika. Poslaním spoločnosti je aj naďalej hľadať lepšie spôsoby

uspokojovania potrieb pre svojich ako aj potenciálnych zákazníkov a odhadovať trendy, ktoré prídu a udržiavať si tak stabilnú pozíciu na slovenskom trhu. Firma bola zapísaná do obchodného registra ako spoločnosť s ručením obmedzeným v časoch, keď vykonávala stavebnú činnosť pod obchodným názvom MARS s.r.o.; podľa stanoveného zákona mala splatené základne imanie vo výške 200 000,- Sk. Po postupnom upustení od činnosti vykonávajúcej stavby a rekonštrukcie opustila svoj štatút s.r.o. a majiteľ pôsobí ako živnostník pod obchodným menom MARS – Meheš. Motiváciou bola legislatívna úprava, ktorá pri takejto forme vychádza v prospech tejto voľby. Ako živnostník ručí za svoje záväzky celým svojim majetkom, čo vo finále predstavuje väčšiu dôveryhodnosť voči obchodným partnerom. Spoločnosti sa darí v priebehu rokov mať stabilný odbyt vďaka ideálnej diverzifikácii zákazníckeho portfólia, veľkoobchod, maloobchod a výrobné podniky. Atraktivitu si udržiava aj spomínanými pomalými obmenami sortimentu. Trh, ktorý firma značne podceňuje je online - doposiaľ nemá plne fungujúci e-shop a funguje len na forme objednávok mailom, či telefonicky.

2.1.3 Hardware a software podniku

Vybavenie hardwarom v podniku je predbežne dokupované a obnovované v prípade potreby, táto potreba väčšinou vzniká v momente pomalej odozvy, prípadne poruchy konkrétneho komponentu. Jednotlivé stanice tak slúžia vyhovujúco v pomere na požiadavky užívateľov.

Sieť je zabezpečená serverom HP Proliant ML350P, na ktorých funguje Windows server 2012. V sieti je diskové pole Raid 1, ktoré obsah zaznamenáva na 2 disky, v prípade výpadku je ihneď k dispozícií kópia. Zálohy prebiehajú na disky alebo HP StorageWorks RDX, teda odoberateľné pevné disky, s ktorými je možné pracovať ako s pevným diskom, alebo iným odoberateľným zariadením. Automatické zálohy na konci prevádzky prebiehajú pomocou HP RDX. Ako záložný zdroj elektrickej energie je používaný APC Smart UPS 750/230.

Väčšina pracovných staníc obsahuje nainštalovaný balík Offce verzie 2007 a 2010 v štandardnej verzii, ktorá obsahuje najčastejšie používané nástroje. Outlook na komunikáciu s okolím, prípadne vo vnútri firmy. Z kancelárskeho balíka sa používa najmä Word, pre prípravu dokumentov, dopyty, ponuky, prípadne zmluvy. Excel sa

využíva ako pomôcka pre tabuľkové prehľady. Antivírusová ochrana je riešená spoločnosťou ESET v podobe balíka Small business security pack.

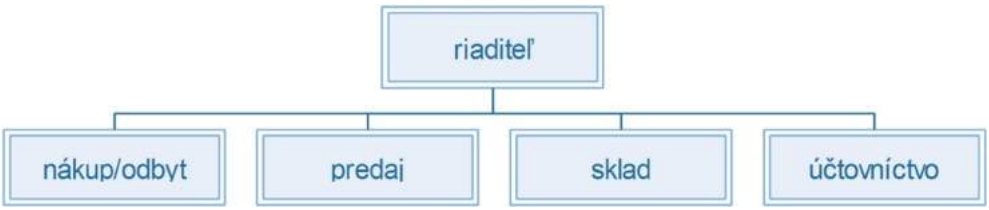
Informačný systém MONEY

Jedná sa o komplexný ERP systém od firmy Cígler software, ktorý okrem bežných účtovníckych a ekonomických funkcií poskytuje aj jednotlivé moduly na kombináciu funkcií. Je možné viesť daňovú evidenciu a účtovníctvo, faktúry a sklady. Umožňuje bohatú mieru prispôsobivosti pre spoločnosti, ktoré potrebujú vlastnosti veľkých ERP systémov, ale investíciu v desiatkach tisíc euro si nemôžu dovoliť. Systém je neutrálny čo sa týka oborov, je vhodný pre živnostníkov, podnikateľov a spoločnosti, ktoré sa zaoberajú aj výrobou, službami, nie len obchodom. Základom systému je prepracovaný adresár a rada agend potrebných na riadenie podniku; napríklad agendy, fakturácia, adresáre s informáciami o dodávateľoch a odoberateľoch, sklady, mzdy, kasa a iné. Systém umožňuje vedenie skladu metódou A aj B a spracovávať mzdy pre neobmedzený počet zamestnancov. Tiež je schopný spracovať dáta podľa filiálok, homebanking, obchodovanie na internete a predaj zásob pomocou vstavanej predajne, alebo pomocou modulu pre offline maloobchodný predaj. V súčasnosti je zakúpená a využívaná licencia MONEY S3 professional, čo pre je pre malé podniky možné chápať ako ERP systém s CRM funkciami, ktorý obsahuje moduly účtovníctvo, adresár, fakturácia, sklady A/B, objednávky, mzdy, majetok a pomocné evidencie. Stanice na pokladni majú zakúpené moduly Kasa profesionál. Systém je založený na spôsobe klient-server, dáta sú umiestené na serveri, kde sa užívatelia pripájajú cez počítačovú sieť pomocou aplikácie, ktorá je nainštalovaná na určitej pracovnej stanici. Zamestnanci podniku v rámci IS využívajú najmä funkcie a možnosti (Money, 2016, online):

- Účtovníctvo (účtovný denník, banka, pokladňa, DPH, záväzky a pohľadávky)
- Fakturácia (vydané a prijaté faktúry)
- Adresár (evidencia obchodných partnerov)
- Sklady (zásoby, príjemky, výdajky, sadzby, cenníky...)
- Objednávky (prijaté a vystavené)
- Mzdy
- Majetok
- Administrácia a bezpečnosť (užívateľské role, užívatelia, zálohovanie)

2.1.4 Organizačná štruktúra

Firma je vedená jej zakladateľom, ktorý je zároveň aj konateľom, jeho hlavnou náplňou je oslovovanie nových obchodných partnerov, tvorba cenových a nákupných stratégií a rozhodovanie nad budúcim vývojom podniku. Zamestnanci sú rozdelení do štyroch oddelení. Každý vedúci oddelenia sa zodpovedá priamo riaditeľovi.



Obrázok 8: Organizačná štruktúra spoločnosti
(Zdroj: Vlastné spracovanie)

Nákup / odbyt – administratívne pracovisko, ktoré sa podieľa na zodpovednosti za toky tovarov, jeho nákup a odbyt pre veľkosklad, komunikácii s dodávateľmi a odoberateľmi, dojednávaní transakcií, objednávok a ich spracovaní do systému, zhotovovaní skladových príkazov. V jeho kompetencii je spracovanie príkazov k výdaju ručným prepisom, zapisovanie zmien pri príjme a výdaji zo skladu, zaznamenávanie úbytkov, kalkulácie cien, opravy v dokladoch.

Predaj – oddelenie maloobchodného predaja.

Sklad – príjem a expedícia tovarov. Vychádzajú z agendy, ktorú obdržia od nákupcov, respektíve predajcov. Má na starosti logistické procesy. Obsluha zákazníkov, fyzická manipulácia s tovarom, vyhľadávanie položiek, obsluha zákazníkov.

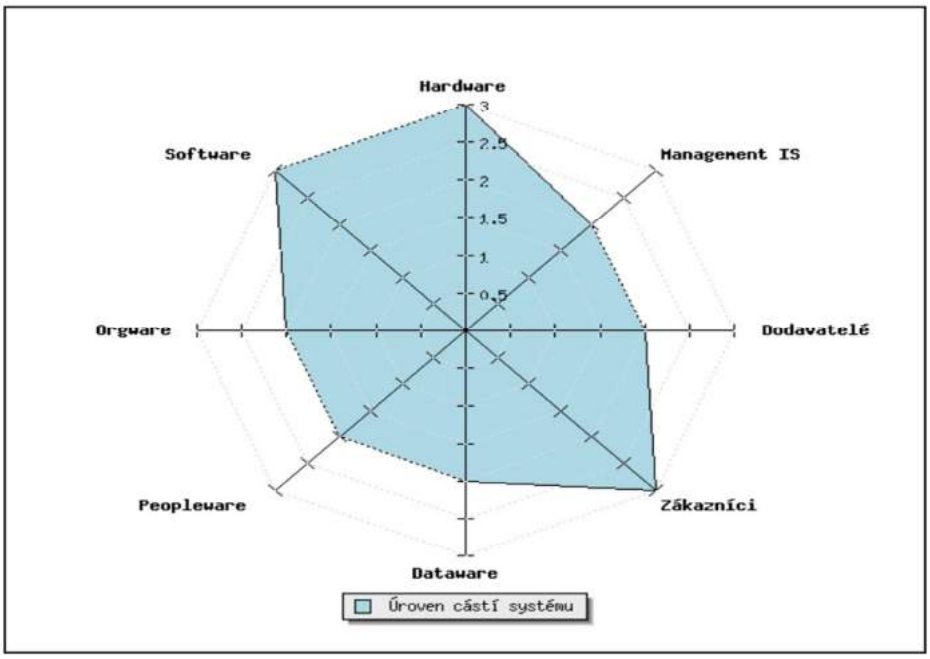
Účtovníctvo – zaisťovanie toku ekonomických informácií, riadi účtovný a finančný systém spoločnosti, dohľad nad financiami, spracovanie agendy v systéme Money.

2.2 Posúdenie vyváženosti IS metódou HOS 8

Pomocou metódy HOS 8, ktorá je voľne dostupná na internetovom portáli www.zefis.cz bolo posúdených 8 kľúčových oblastí informačného systému, ktoré sú východiskom posúdenia vyváženosti informačného systému. Ide o návrhy založené na vyhodnotení dotazníkového šetrenia, ktoré bolo vykonané konateľom podniku. Výstupom je grafické zobrazenie. Výsledky majú informačnú podobu, slúžia ako podnet pre návrhovú časť.

1) Posúdenie jednotlivých oblastí

Každá os predstavuje jednu oblasť informačného systému, ktoré znázorňujú jednotlivé úrovne. Každá oblasť je hodnotená v rámci štyroch úrovni, 1 – zlá, 2 – skôr zlá, 3 – skôr dobrá, 4 – dobrá.



Obrázok 9: Posúdenie skúmaných obastí
(Zdroj: Vlastné spracovanie podľa výsledkov Zefis.cz)

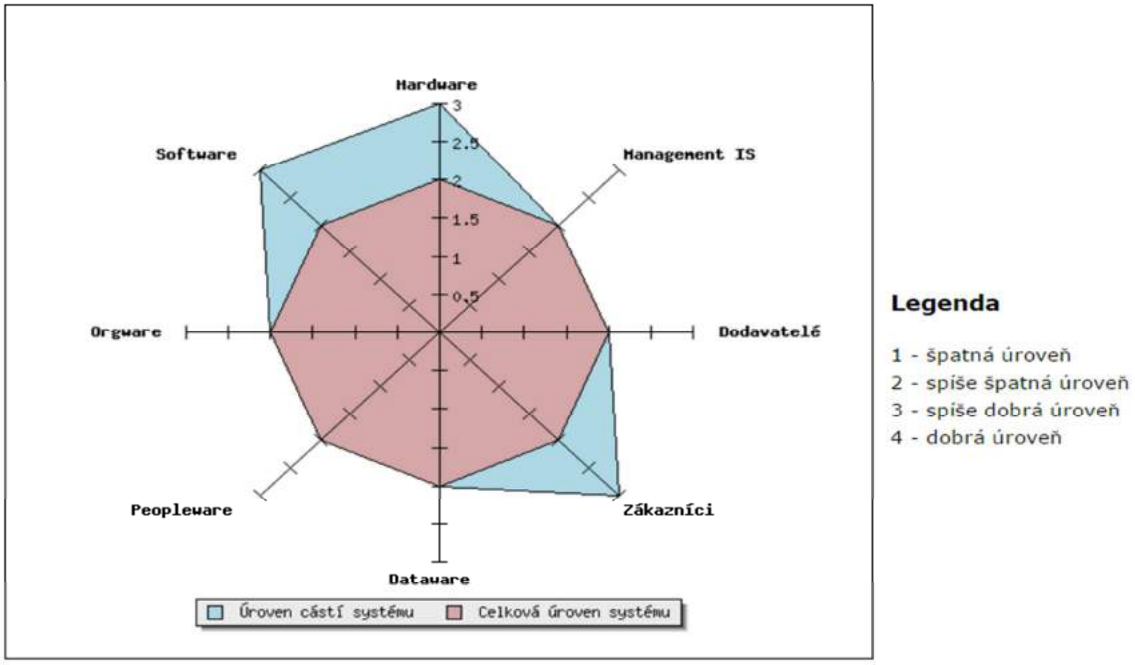
Tabuľka 1: Posúdené oblasti

Oblasť	Body	Úroveň
hardware	3	skôr dobrá úroveň
software	3	skôr dobrá úroveň
orgware	2	skôr zlá úroveň
peopleware	2	skôr zlá úroveň
dataware	2	skôr zlá úroveň
zákazníci	3	skôr dobrá úroveň
dodávateľia	2	skôr zlá úroveň
management IS	2	skôr zlá úroveň

(Zdroj: Vlastné spracovanie podľa výsledkov Zefis.cz)

2) Celkový stav informačného systému

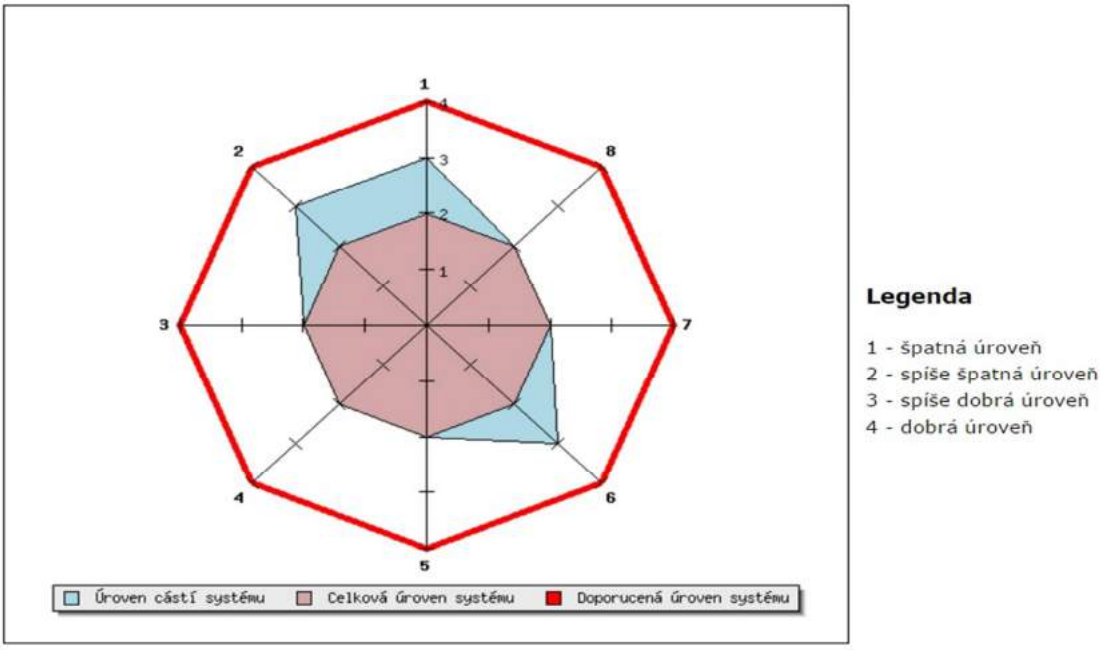
Celková úroveň informačného systému firmy je vyhodnotená ako skôr zlá (hodnotenie 2). Výsledok má túto hodnotu práve preto, že úroveň celého informačného systému je daná najnižšou úrovňou, ktorá bola zistená u posudzovaných oblastí.



Obrázok 10: Celkový stav IS
(Zroj: Vlastné spracovanie podľa výsledkov Zefis.cz)

3) Doporučený stav informačného systému

Z vykonanej analýzy vyplýva, že doporučená úroveň všetkých oblastí informačného systému by na základe jeho dôležitosti pre podnik mala byť na stupni 4 – dobrý. Doporučený stav je navrhnutý na základe respondentovej odpovede, že informačný systém je pre činnosť podniku nevyhnutný. Doporučená úroveň systému je vyznačená červenou farbou, ktorý je potrebné považovať za minimálnu požadovanú úroveň. Stupeň 2 – skôr zlý je pre podniky, ktoré dokážu fungovať bez informačného systému.



Obrázok 11: Doporučený stav IS
(Zdroj: Vlastné spracovanie podľa výsledkov Zefis.cz)

4) Vyhodnotenie

Skúmaný informačný systém má nižšiu úroveň ako je stanovená očakávaná na základe dôležitosti systému pre podnik. Veľký rozdiel medzi skutočnosťou a očakávaným stavom je daný potrebou informačného systému pre chod celej organizácie. Skutočná úroveň zobrazená analýzou je v oblastiach management IS, dodávatelia, dataware, peopleware, orgware, skôr zlá. Za skôr dobré sa považujú software, zákazníci a hardware. Súčasťou vyhodnotenia metódou HOS 8 je komentár a odporúčania, na ktoré prvky je potrebné sa sústrediť. Na základe pozorovania v rámci podniku a vyhodnotenia metódou boli zistené nasledujúce závery:

Hardware

Na základe odpovedí na otázky, existuje vo firme určitá kontinuita v obnove techniky za novú, systémy bežia preto dobre bez citeľných výpadkov, veľkej odozvy. Nutnosť obmeny by sa však mala týkať systému ako celku. Je citeľné, že obchod resp. pokladňa beží na starších počítačoch a doba odozvy je dlhšia ako by v dnešnej dobe mala byť a efektivita sa tak rapídne znižuje aj s počtom obslúžených zákazníkov. Rýchlosť a stabilita siete je však pre potreby podniku dostačujúca. Fyzická ochrana je

na dostačujúcej úrovni, počítače sú počas pracovného dňa pod dohľadom a mimo pracovnej doby uzamknuté v priestoroch so zabezpečovacím systémom. V blízkej dobe je plánovaný nákup kamerového systému. Nákupy v najbližšej dobe sa budú týkať hlavne rozširovania systémov, kde bude dôležité vykonávať nákup po overení kompatibility so súčasnou technikou.

Software

Software poskytuje funkcie, ktoré sa využívajú a sú potrebné. Systém je prehľadný a užívatelia sú na jeho rozhranie zvyknutí. Komplikácie nastávajú v prípade zrútenia systému, kedy musí prísť externý dodávateľ a systém tak zostáva nečinný. Určitá nespokojnosť zamestnancov vychádza aj z toho, že nie všetci sú na toľko technicky zdatní aby rozumeli chybovým hláseniam, a v prípade potreby zmeny kompetencie reagovať okamžite na požiadavku. Postupom času nastali potreby niektorých funkcií, ktoré systém už obsahoval - bol obstaraný aj funkciami ktoré sa dlhodobo nevyužívali. Celkovo prevláda so systémom spokojnosť; aby sa predišlo problémom pri aktualizáciách, ten sa aktualizuje až s určitým oneskorením.

Orgware

V podniku neexistujú postupy a bezpečnostné pravidlá informačného systému, ktoré by definovali s akými dátami a dokumentmi má pracovať, či má mať na počítači heslo a obmieňať ho, či môže svojvoľne pripájať pamäťové média resp. inštalovať svojvoľne programy, alebo meniť nastavenia podľa svojich predstáv. O tom ako pracovať s informačným systémom sú väčšinou len poučení pri preberaní do užívania, prípadne sa dozvedia od skúsenejšieho užívateľa. Existuje povedomie aby sa vyššie spomínané udalosti nevyskytovali, to však nezabráni nikomu vo vykonaní záškodnej činnosti. Dodržiavaním a sledovaním bezpečnosti a prevádzky sa vo firme nikto nezaoberá. Do budúcnosti by bolo vhodné vypracovať pravidlá o prevádzke a bezpečnosti informačného systému, vrátane pravidelných školení. Firma by mala vykonať minimálne fyzické úpravy pracovných staníc tak, aby nebolo možné sa dostať do niektorých častí systému a upraviť niektoré práva na jednotlivých úrovniach, ktoré umožňuje aj samotný software.

Peopleware

Pracovníci nie sú zaškolení na úlohy na pravidelnej báze, ale len na úrovni pri preberaní programu do užívania. Ostatné informácie je potrebné si individuálne pýtať pri údržbe systému od externého pracovníka. V procesoch, zdá sa, si vedomosti odovzdávajú pracovníci navzájom a riadia sa svojimi skúsenosťami a radami. Je žiaduce, aby sa zaviedlo pravidelné školenie pre prácu s informačným systémom. Pracovníci na nižších úrovniach svoje základne úlohy vykonávať zvládajú a zastupiteľnosť pri ich úkonoch nie je problémom. Nízka zastupiteľnosť je u ekonómky a účtovníčky, ktorá si však svoju agendu môže dopracovať a faktúry je schopný uhrádzať aj nákupca. Veľmi ťažko nahraditeľní pre chod obchodu sú nákupcovia, ktorí disponujú vedomosťami o sadzbách a komunikujú s vonkajším prostredím. To vedie v niektorých prípadoch k neefektívnosti, keď pracovníci z nižších pozícií nevedia zastúpiť tých, nad nimi nadriadených. V spoločnosti chýba zamestnanec, ktorý by mal na starosti definovanie informačnej stratégie a celkovú zodpovednosť za beh IS. Dodržiavanie pravidiel nie je kontrolované a bolo by vhodné mať systém kontroly a prípadných sankcií.

Dataware

Pracovníci majú k dispozícií všetky dáta, ktoré potrebujú k práci, nesú za ne zodpovednosť a mali by mať bližšie určené kedy a aké dáta je potrebné do systému zaviesť. Táto zodpovednosť je neformálna, ale uvedomujú si ju. V podniku prebieha na konci dňa automatická záloha dát z prevádzkových jednotiek na serveri. Tieto dáta nie sú v oddelenej miestnosti. Zálohy na lokálnych počítačoch jednotlivých pracovníkov vykonávané nie sú. V skutočnosti sa však jedná o dáta mimo účtovníctva, prípadne pohybov na sklade, ktoré sú nahraditeľné a nemajú kritický vplyv na chod spoločnosti. Dáta aj napriek zálohe sú však vystavené hrozbám prostredníctvom infikovania počítačov, alebo vnútornej hrozbe smerom od zamestnancov. Bolo by vhodné skontrolovať zabezpečenie jednotlivých počítačov a určiť pravidlá a postupy pri používaní dát zo systému - kto môže pracovať s akými dátami. Nikto by nemal získať prístup k dátam, ktoré nepotrebuje k vykonávaniu svojej činnosti.

Zákazníci

V podniku nie sú definované ciele informačného systému, ani metriky, ktorými by sa meralo, ani vyhodnotenie ako informačný systém plní svoju rolu, prípadne ako sú s ním

užívatelia spokojní. Nie je ani skúmané, čo od systému zákazníci (pracovníci) očakávajú. Zaviesť by sa mohlo minimálne vytvorenie priestoru pre diskusiu a návrhy, a vedenie by malo reflektovať tieto podnety. Užívatelia informačného systému z neho dostávajú konkrétne informácie, ktoré sú potrebné pre výkon ich práce. Pokiaľ je potrebné zistiť ďalšie informácie, je možné sa dopytovať u vyššie postaveného pracovníka. Hardwarové a softwarové nastavenie má rýchlu odozvu vďaka jeho aktuálnosti. V prípade, že pracovník potrebuje získať iné dáta, ktoré nie sú obsiahnuté v prostredí, s ktorým pracuje, môže dochádzať k časovým prestojom. Užívateľ v takom prípade získava výstupy z rôznych komunikačných kanálov.

Dodávatelia

Táto oblasť trpí zásadnými nedostatkami. Vo firme by sa malo začať uvažovať s možnosťou vlastného pracovníka na úrovní IT, prípadne správcu siete, ktorý by zabezpečoval chod IS a technické opravy, aby sa zmenšil čas, ktorý je potrebný na nápravu. Momentálne zabezpečuje technickú podporu konateľ a pracovník s najväčšími skúsenosťami, ale nejedná sa o odborníka. Užívateľská podpora sa využíva iba v kritických situáciách, v prípade keď nastane výpadok. Spoločnosť nemá uzavretú SLA zmluvu s dodávateľom, z toho pramení hlavná nespokojnosť so službami. Pri dodávateľovi neexistuje účinný spôsob ako zabezpečiť, aby podával kvalitný servis. Problémom je aj čakanie na externého pracovníka v prípade potreby. Je možné kontaktovať ho e-mailom, prípadne telefonicky, ale z dôvodu neodbornosti užívateľov tieto kanály nie sú nápomocné. Z toho pramení určitá nespokojnosť s dodávateľom, ide však aj o problém firmy, ktorá by si mala vedieť poradiť v niektorých situáciách aj bez dodávateľa.

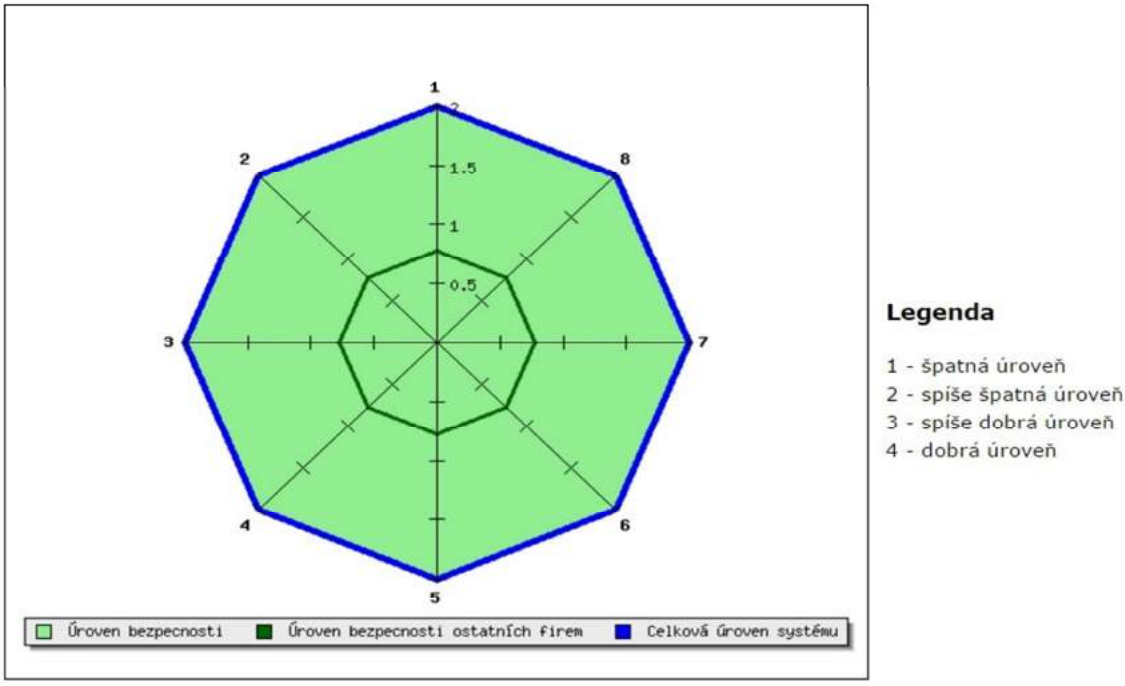
Management IS

Podnik nemá vypracovanú informačnú stratégiu. Je potrebné stratégiu vytvoriť, aby systém neobsahoval toľko nedostatkov, ktoré majú vplyv na výslednú efektivitu, nákladovosť a budúci vývoj systému. Vedenie firmy nesleduje ani nekontroluje dodržiavanie pravidiel prevádzky a bezpečnosti. Informačný systém však považuje za nevyhnutnosť, čo pomáha dosahovať určité ciele v rámci obchodnej činnosti. Napriek tomu nevníma naplno potenciál a význam informačných systémov pre činnosť

a rozvoj. Vedenie si však uvedomuje určité významy tejto analýzy, preto by sa mali jej výsledky zapracovať pri tvorbe dokumentu stratégie.

5) Informačná bezpečnosť

Táto časť sa zaoberá odhadom informačnej úrovne bezpečnosti podniku. Z prieskumu sa došlo k záveru, že súčasťou stratégie podniku nie je informačná bezpečnosť a nie je ani súčasťou informačného systému. V spoločnosti sa neobmieňajú pravidelne heslá, nie sú zabezpečené zálohované dáta, nie sú zadefinované prístupy a právomoci, nemyslí sa na externé hrozby. Existuje tak priestor na zlepšovanie. Úroveň bezpečnosti bola vyhodnotená ako skôr zlá (hodnota 2) a je zobrazená zelenou oblasťou v grafe. Celková úroveň informačného systému je znázornená silnou modrou čiarou.



Obrázok 12: Odhad bezpečnostnej úrovne
(Zdroj: Vlastné spracovanie podľa Zefis.cz)

2.3 Analýza efektívnosti IS pomocou Zefis

Na posúdenie efektívnosti informačného systému vo firme a jeho slabých miest bol opäť využitý portál Zefis (www.zefis.cz). Pre tento prieskum bolo vyplnených celkovo 6 dotazníkov od zamestnancov, ktorí pravidelne využívajú informačný systém. Dotazník obsahuje 58 otázok vzťahujúcich sa na tieto oblasti:

- Váš informačný systém,

- Vaši zamestnanci,
- Úroveň podpory,
- Úroveň riadenia,
- Efektívnosť IS,
- Bezpečnosť IS,
- Chápanie IS ako služby.

Podľa odporúčaní portálu Zefis bol vyplnený postačujúci počet dotazníkov na posúdenie celej organizácie. Výsledky môžu byť brané za celú organizáciu, aj keď môže dochádzať k menším a málo pravdepodobným odlišnostiam. V odpovediach na základné otázky sa dospelo k 100% zhode, ktorá odráža skutočný stav a je možné považovať výsledky za dôveryhodné.

Tabuľka 2: Základné údaje dotazníkového prieskumu efektívnosti pomocou Zefis

Veľkosť vašej firmy:	10 až 49	(6/6)
Oblasť podnikania:	Obchodná firma	(6/6)
Krajina:	Slovenská republika	(6/6)
Orientačný počet PC:	10 až 49	(6/6)

(Zdroj: Vlastné spracovanie podľa výsledkov Zefis.cz)

Vo vyhodnoteniach v nasledujúcich kapitolách sú používané tri najčastejšie odpovede, preto sa súčet percent nemusí rovnať 100.

Posudzovaný informačný systém

Táto časť vypovedá o povedomí konkrétneho IS, ktorý zamestnanci spoločnosti pri svojej činnosti využívajú najviac. Na otázku aký informačný systém používate, odpovedalo 83% možnosť malý informačný systém, čo predstavuje systém Money. Zvyšok respondentov odpovedal, že nevie. Spoločnosť si všetok využívaný informačný systém nakupuje a využíva tak hotové riešenia.

Staroba informačného systému je dôležitým prvkom v rámci efektívnosti. Príliš starý informačný systém by mohol spôsobovať nevyhovujúcu podporu jednotlivých procesov v podniku a pomalú odozvu. Záleží však aj na okolnostiach - nie vždy je starý systém nekvalitnejší než nový. 66% uviedlo 5 – 10 rokov. Systém už presahuje päť rokov, je však stále podporovaný zo strany výrobcu.

V otázkach silných a slabých stránok informačného systému z pohľadu používateľov sa ukázalo, že silné stránky sú individuálne a môžu byť aj skreslené schopnosťou práce s PC, prípadne výkonu HW na danej pracovnej stanici.

Tabuľka 3: Silné a slabé stránky informačného systému

Silné stránky		Slabé stránky systému	
Technika	37 %	Podpora	50 %
Rýchlosť odozvy/spracovanie	25 %	Programové vybavenie	20 %
Nijaká z možností	25 %	Rýchlosť odozvy/spracovanie	20 %

(Zdroj: Vlastné spracovanie podľa výsledkov Zefis.cz)

Zo slabých stránok je vidno všeobecné povedomie o zlej prípadne neexistujúcej podpore, ktorá trápi takmer polovicu zamestnancov.

Zamestnanci

Prieskum bol vykonaný na štruktúre pracovníkov tak, aby bol braný ohľad na ich profesijné zaradenie. Vo výskume boli zúčastnení zástupcovia z každej skupiny zamestnancov. Zo zistených informácií vyplýva, že 33% boli riadiaci pracovníci v hlavných procesoch firmy, 33% výkonní pracovníci v hlavných procesoch a po 16% výkonní a riadiaci pracovníci z podporných procesov firmy.

Pretože sa jedná o obchodnú spoločnosť orientovanú na strojárstvo, všetci pracovníci okrem účtovníkov majú vzdelanie technického zamerania a okrem účtovníkov má 83% dosiahnuté najvyššie vzdelanie stredoškolské, čo je v rámci trhu a regiónu bežné. Najviac zamestnancov, 66% je vo veku od 21 – 41 rokov. Taktiež 66% pracuje v spoločnosti viac ako 3 roky. Náklady na takýchto pracovníkov sú aj rádovo nižšie.

Tabuľka 4: Vzťah zamestnancov k PC

Aký majú zamestnanci vzťah k počítačom?	
Dobrý, viem s ním dobre pracovať, využívam ich vo väčšine prípadov.	66 %
Neutrálny, viem s nimi pracovať na požadovanej úrovni.	33 %

(Zdroj: Vlastné spracovanie podľa výsledkov Zefis.cz)

Vzťah väčšiny respondentov k počítačom je dobrý a vedia ovládať zverené informačné systémy, predpokladá sa, že tí čo uvádzajú negatívny vzťah k počítačom, s nimi neprichádzajú tak často do styku a nie je na nich z pohľadu IS kladený vysoký nárok.

Vo firme existuje predpoklad schopnosti sa pomerne efektívne naučiť novým funkciám, systémom, keďže polovica pracovníkov používa IS väčšinu pracovného dňa. Vo firme však neexistuje nijaká forma vzdelávania pracovníkov v oblasti IS a je pravdepodobné, že zamestnanci konkurenčných firiem vedia svoje systémy, pokojne aj rovnaké, využívať lepšie.

Tabuľka 5: Čas využívania informačného systému

Ako často používate informačný systém?	
Väčšinu pracovného dňa.	50 %
Niekoľkokrát denne.	33 %

(Zdroj: Vlastné spracovanie podľa výsledkov Zefis.cz)

Podpora

Tieto otázky skúmajú akú podporu pri práci s informačným systémom majú zamestnanci k dispozícii a ako sú s ňou spokojní, je to veľmi dôležitý faktor. Kvalitná podpora zvyšuje efektívnosť celého systému a naopak.

Pri skúmaní spokojnosti respondentov s podporou informačných systémov bola zistená prevládajúca nespokojnosť s touto oblasťou, takmer až povedomie, že v podniku nijaká neexistuje.

Tabuľka 6: Spokojnosť s podporou informačného systému

Ste spokojní s podporou informačných systémov?	
Rozhodne nie, nemáme žiadnu podporu.	50 %
Máme podporu, ale neodpovedá potrebám.	33 %

(Zdroj: Vlastné spracovanie podľa výsledkov Zefis.cz)

Tento výsledok je veľmi negatívny a aj samotní zamestnanci cítia, že v prípade užívateľskej podpory, ktorú zastrešuje externá firma sa ich produktivita znižuje.

Technická podpora je zaisťovaná prípad od prípadu, kedy ju v rámci možností zvláda pracovník, ktorý ale nie je primárne zamestnaný na to aby ju vykonával. Problémy tak

rieši pomaly, nemôže sa venovať svojej práci a výsledok nikdy nie je istý. 66% zamestnancov sa v prípade technických problémov dopytuje na spomínaného kolegu.

Doby technických opráv sa líšia od závažnosti prípadu, 66% respondentov ale uvádza dobu opravy menšiu ako jeden deň. 16% menej než 4 hodiny. V rámci inštalácie, alebo zmeny programu bola doba u 66% dopytovaných respondentov 1 až 2 dni, čo už predstavuje vážny výpadok pracovnej sily. 16% respondentov dokonca uviedlo dobu 2 až 5 dní. V tomto prípade hrá rolu aj obsadenosť a voľnosť externého pracovníka, ktorý nepríde vo všetkých prípadoch okamžite. Celkovo tak v otázke spokojnosti s užívateľskou podporou prevláda nespokojnosť.

Tabuľka 7: Spokojnosť s užívateľskou podporou

Ste spokojní s užívateľskou podporou?	
Rozhodne nie.	50 %
Máme podporu, ale neodpovedá potrebám.	50 %

(Zdroj: Vlastné spracovanie podľa výsledkov Zefis.cz)

Úroveň riadenia

Otázky z tejto skupiny sú zamerané na oblasť, ktoré môžu vytvárať komplikácie v riadení firmy. Konkrétne skúma, či v podniku pôsobí CIO (chief information officer), teda manažér zodpovedný za IS. V skúmanej firme nie je, čo zodpovedá podobným podnikom, čo do veľkosti, v obore. Všetci zamestnanci sledovaného podniku uviedli, že si nie sú vedomí niekoho na obdobnej pozícii.

Otázky, ktoré sa týkali podnikovej a informačnej stratégie ukázali, že 50 % respondentov analyzovanej firmy si nie je vedomá stratégií podniku a jeho cieľov. Ostaných 50 % uviedlo, že vie len čiastočne. Bez znalosti podnikovej stratégie, sa však len veľmi ťažko môže naplniť cieľ alebo vízia majiteľov. U znalosti informačnej stratégie to bolo v odpovediach rovnako.

Znalosť podnikovej stratégie je veľmi úzko prepojená s informovanosťou o plnení cieľov podniku a podiele na dosiahnutom výsledku pracovníkoV. Aj v tomto prípade má analyzovaný podnik veľké nedostatky. 83% respondentov uviedlo, že bývajú o plnení cieľov firmy informovaní len občas a 66% respondentov nebýva informovaných o ich vlastnom pričinení k dosiahnutým výsledkom. Táto problematika

je dôležitá z pohľadu firemného ducha a sunáležitosti s firmou, preto tí, ktorí sú v týchto ohľadoch informovaní, zvyšujú vďaka motivácii firemnú efektivitu.

Oblasť úrovne riadenia obsahujú aj pravidlá pre prácu s informačným systémom. Tieto pravidla by mali definovať zodpovednosť pracovníkov za dáta, určovať aké dáta a kedy môžu vkladať do systému, aké funkcie môžu využívať a iné.

Tabuľka 8: Existencia pravidiel pre prácu s informačným systémom

Existujú vo Vašej firme pravidlá pre prácu s informačný systémom?	
Nemáme žiadne pravidlá, alebo nich nič neviem.	50 %
Viem že existujú, ale ja o nich nič bližšieho neviem	33 %
Áno, existujú, ale nie sú príliš kontrolované alebo vyžadované	16 %

(Zdroj: Vlastné spracovanie podľa výsledkov Zefis.cz)

Efektívnosť informačného systému

Oblasť skúma efektívnosť informačného systému z hľadiska nákladov vynaložených na jeho prevádzku, či sú adekvátne, a ktoré časti informačného systému by mohli pracovníkom viac uľahčiť ich prácu.

- **Môžu zamestnanci vykonávať svoju prácu bez IS ?**

Pomocou tejto otázky je zisťovaná dôležitosť informačného systému pre jednotlivých pracovníkov podniku. Na základe čoho budú tvorené niektoré ďalšie odporúčania. Väčšina respondentov (66%) uviedla, že by svoju prácu bez IS vykonávať rozhodne nemohli, 16% následne by mohlo vykonávať svoju činnosť s malými obtiažami a rovnako 16% len s veľkými obtiažami.

- **Mohla by firma fungovať bez IS ?**

Táto otázka skúma, ako je dôležitý podľa pracovníkov informačný systém a či by firma mohla ďalej vykonávať svoju zárobkovú činnosť alebo nie. 83% respondentov uviedla, že by podnik bez informačného systému v žiadnom prípade nefungoval, ostatní sa priklonili k možnosti neviem.

- **Mohol by IS viac pomáhať zamestnancom a zlepšiť tak procesy firmy ?**

V tomto bode je zachytené, do akej miery je informačný systém v zhode s potrebami pracovníkov. Podľa odpovedí si 83% myslí, že by informačný systém mohol lepšie

napĺňať jednotlivé potreby. Pričom 50% si myslí, že by sa čiastočne zlepšil pracovný výkon. 16% respondentov uvádza, že by mohli byť zlepšené informácie potrebné k rozhodovaniu a 16% si myslí, že by sa zvýšil pracovný výkon významne.

Z celkového pohľadu, ktorý môže dávať odpovede na niektoré predchádzajúce výsledky, sme dospeli k zisteniu, že v podniku absentujú školenia pre prácu s informačným systémom. Nikto nikdy na žiadnom školení nebol. Zamestnanci tak môžu mať pocit, že IS nenapĺňa ich požiadavky a pritom len neovládajú funkcie IS.

Tabuľka 9: Absolvované školenia

Absolvovali ste školenie, alebo vám bolo ponúknuté?	
Nie, neabsolvoval ale bolo mi ponúknuté	33 %
Nie, neabsolvoval, nebolo mi ponúknuté	66 %

(Zdroj: Vlastné spracovanie podľa výsledkov Zefis.cz)

Pri skúmaní, či existuje záujem o školenie však respondenti z 83% odpovedali kladne. Usporiadanie školenia by mohlo viesť k zvýšeniu efektívnosti využívaniu systému.

Bezpečnosť informačného systému

Na otázku, či existujú bezpečnostné pravidlá a či ich pracovníci dodržiavajú alebo či vedenie vyžaduje ich dodržiavanie, všetci zúčastnení odpovedali, že nemajú žiadne pravidlá, alebo o nich nevedia.

V časti, kde sa skúma prístup do počítačovej siete pre zamestnancov alebo pre verejnosť (či je možne pripájať svoje súkromné zariadenia do siete), čo môže vytvárať pre sieť riziko, odpovedali všetci jednoznačne, že nie. Zabezpečenia na týchto úrovniach však vo firme nie sú. Vzhľadom na to, že lokálna sieť je vedená káblom a nie bezdrôtovo, nie je veľa možností, kde by sa dalo pripojiť.

Na úrovni vnímania rizík ako by užívateľ reagoval na ponuku neznámeho dialógového okna s ponukou neškodne sa tváriacej aplikácie, by na žiadosť o povolenie prístupu neznámeho programu na ich počítač reagovali v podobe zatvorenia okna prehliadača.

V časti zálohovania a otázky, či majú pracovníci na svojich počítačoch uložené dáta a ako sú chránené pred poškodením, alebo zničením, teda akým spôsobom prebieha ich záloha boli odpovede nasledovné.

Tabuľka 10: Spôsob zálohovania dát

Niekto iný.	66 %
Nikto, ale môj PC neobsahuje dáta, ktoré vytváram a používam k práci.	16 %
Ja sám.	16 %

(Zdroj: Vlastné spracovanie podľa výsledkov Zefis.cz)

V prípade otázky, aký by bol dopad v prípade poškodenia a ak dlho by trvalo obnovenie dát odpovedalo 50 %, že by im obnova trvala 1 – 2 dni, ďalších 16% by odpovedalo že by bola zničená všetka práca a neexistovala k nim záloha a 16 % respondentov odpovedala 2 – 5 dní.

Výsledky tejto časti vedú k záverom, že dáta sú zálohované, ale len niektoré a najčastejšie na rovnakom počítači a disku. Len minimum záloh je ukladaných na iné miesta.

Na otázku vnímania bezpečnostnej politiky, či užívatelia používajú heslá a ako ich chránia, boli odpovede nasledujúce:

- Pamätám si ich, odpovedalo 50%
- Hesla nepoužívam / mám ich zapísane niekde pri PC, odpovedalo 16%

Dotazník vôbec neskúmal zložitosť zvolených kombinácií pri tvorbe hesiel. Pri vychádzaní z dotazníkov a vzťahu k IS, sa dá predpokladať, že hesla budú skôr jednoduchšieho charakteru. Dopad straty dát by v 50% znamenal stredne veľké škody. Zamestnanci sú presvedčení, že strata dát z ich PC by nemohla spôsobiť firme veľké problémy. 33% vníma stratu dát ako veľmi vážnu, ktorá by spôsobila obrovské škody.

V ďalších otázkach prístupov a rizík zhodne 83% respondentov odpovedalo, že si môžu pripojiť externé pamäťové média, nainštalovať program a ísť voľne na internet. V podstate ktokoľvek, kto je na úrovni vyššej ako predavač predstavuje neobmedzené riziko pre informačný systém. Tu je veľký priestor na zavedenie pravidiel a obmedzení.

Chápanie IS ako služby

Táto časť prieskumu skúma, či pracovníci chápu informačný systém ako službu, podporný proces svojej práce, alebo ako integrálnu súčasť svojich procesov. Toto chápanie je dôležité pre úvahy nad možným outsourcingom informačného systému, jeho častí, alebo podpory pracovníkov. Odpovede naznačujú, že väčšina (83%) z pracovníkov si nevie predstaviť zaistenie prevádzky informačného systému mimo podnik a prenajímať si ho od dodávateľa. Vyplývať to môže rovnako aj z neexitujúcej skúsenosti (83%) z outsourcingu u respondentov.

2.4 SWOT analýza súčasného IS

Podkladom pre tvorbu SWOT analýzy bol zistený aktuálny stav vyhodnotený dotazníkovým šetrením, výsledky analýzy metódou HOS 8, informácie získané z rozhovorov so zamestnancami a vlastné pozorovanie. V nasledujúcej matici sú tak identifikované silné, slabé stránky, príležitosti a hrozby.

Tabuľka 11: SWOT analýza

Interné faktory	
SILNÉ STRÁNKY	SLABÉ STRÁNKY
Kvalita hardware	Úroveň podpory
IS pripravený na nadstavby	Neexistujúce predpisy pre prácu s IS
Voľné finančné prostriedky	Slabá vzdelanosť užívateľov IS
	Neexistujúca pozícia správcu siete
	Zabezpečenie informácií
	Nevykonáva sa kontrola IS
	Nízka zastupiteľnosť
Externé faktory	
PRÍLEŽITOSTI	HROZBY
Vznik pracovnej pozície správcu sieti	Pomalá reakcia na nové príležitosti
Vytvorenie smerníc pre IS	Únik informácií
Využitie nových modulov systému	Strata fyzických dát
Zavedenie internetového obchodu	Bezpečnostné rizika

(Zdroj: Vlastné spracovanie)

2.5 Analýza rizík

Na základe výskumu analýz za použitia portálu Zefis a vlastného pozorovania sa odhalili nedostatky informačného systému spoločnosti. V nasledujúcej kapitole budú posúdené riziká plynúce z týchto nedostatkov.

Oblasť hardware

Oblasť technických prostriedkov odhalila nasledujúce, možné slabiny:

- Ako spomína metóda HOS 8 systém je práve taký výkonný ako najslabšia jeho časť, nestabilita aktuálnosti HW spôsobuje, že niektoré stanice trpia väčšou odozvou. Možné riziko: neefektívnosť práce.
- Chýbajúce prostriedky, ktoré by pomáhali k lepšiemu využívaniu IS: Pomalá odozva.
- Vychystávanie objednávky, alebo obsluha zákazníka prebieha papierovou formou a nie je automatizovaná. Možné riziko: Strata dát.
- Skúsenosť prezradila, že technika sa nakupuje bezhlavo a jej kúpa vyúsťuje v nekompatibilitu systémov. Možné riziko: nefunkčnosť častí IS.

Oblasť software

Zistené nedostatky a riziká v oblasti software:

- Chybové hlásenia, ktorým užívatelia nerozumejú a nenavedú ich k riešeniu problému. Možné riziko: pochybenie z dôvodu nezrozumiteľnosti
- IS má funkcie, ktoré sa v podniku nevyužívajú. Bolo by vhodné, aby školenie obsiahlo celú využiteľnosť IS. Možné riziko: Nevyužívanie funkcií, zle stanovené ceny, pomalá odpoveď.
- Aktualizácie softwaru bývajú často nevyskúšané v ostrej prevádzke a v prípade inštalácie spôsobujú chyby. Možné riziko: strata dát.

Oblasť orgware

Zistené nedostatky a riziká v oblasti orgware:

- Neexistencia stanovených pravidiel a vyvodzovania dôsledkov bezpečnostnej prevádzky IS a zaobchádzania s dátami - hrozí ich strata. Možné riziko: nedodržiavanie bezpečnosti, nevymožiteľnosť zodpovednosti.
- Niektoré stanice majú neobmedzený prístup na internet a tak môžu sťahovať neobmedzený obsah a ich PC byť napadnuté. Možné riziko: infikácia vírusmi.
- Možnosť pripájania vlastných pamäťových zariadení, ako napríklad USB kľúčov. Možné riziko: riziko úniku dát a zavírenia IS.
- Možnosť svojvoľnej inštalácie softwaru a hrozba pokuty. Možné riziko: trestnoprávna zodpovednosť.

Oblasť peopleware

Zistené nedostatky a riziká v oblasti peopleware:

- Zamestnanci s technickým vzdelaním a bez vzťahu k PC majú problémy s ovládaním svojich činností, problémom sú neexistujúce školenia. Možné riziko: chybné spracovanie úloh.
- Nízka zastupiteľnosť pracovníkov na vedúcich pracovných pozíciách, ako napríklad účtovníčka, nákupca. Možné riziko: neukončenie procesov.
- V podniku nie je osoba, ktorá by mala na starosti kontrolu využívania IS. Pracovníci sa tak môžu rozhodovať svojvoľne. Možné riziko: vypracovanie úlohy v rozpore s cieľmi organizácie kvôli nedostatočnej kontrole.
- Spracovanie objednávok a ich dokumentácia je vykonávaná manuálne. Možné riziko: chybný výstup pre odoberateľa.
- Informácia o objednávke sa presúva medzi dvoma oddeleniami. Možné riziko: vystavenie chybnej faktúry.
- Deficit znalostí zamestnancov vedie k nepripravenosti na neočakávané udalosti, napríklad pri neštandardnej požiadavke zákazníka. Možné riziko: Chybné spracovanie neštandardnej úlohy.

- Zásadným nedostatkom sa ukazuje byť absencia človeka, ktorý by mal na starosti IT, ktorý by mohol zabezpečovať podporu pre pracovníkov vo viacerých oblastiach. Možné riziko: nedostatočná podpora.

Oblasť dataware

Zistené nedostatky a riziká v oblasti dataware:

- Záloha veľkých dát prebieha, no následne sú iba položené vedľa pracovnej stanice. Možné riziko: krádež alebo fyzické znehodnotenie veľkých dát.
- Záloha pracovných dát, ktoré využívajú k svojej činnosti pracovníci na jednotlivých pracovných staniciach sa nevykonáva. Možné riziko: strata nezálohovaných malých dát.
- Voľný prístup do prostredia internetu a prístup k dátam, ktoré nepotrebuje pracovník k svojej činnosti. Možné riziko: krádež dát.
- Voľný fyzický prístup k dátam, ktoré pracovník nepotrebuje k svojej činnosti. Možné riziko: krádež dát.
- Spracovanie objednávok a ich dokumentácia je vykonávaná manuálne. Možné riziko: nenávratne stratené dáta.
- Dávkové spracovanie objednávok - na konci dňa u nákupcov po ich kompletizácii vzniká nesúlad skladových zásob. Možné riziko: nezrovnalosti stavov.

Oblasť zákazníci

Zistené nedostatky a riziká v oblasti dataware:

- V podniku neexistuje informačná stratégia, ktorá by definovala ciele. Možné riziko: nevyužitie potenciálu IS.
- Vedenie nevedie diskusiu s užívateľmi a tak sa neberú do úvahy ich potreby a námety. Možné riziko: zníženie produktivity.
- Celkový čas vybavenia objednávky je z podstatnej miery závislý na výkone, pamäti, koncentrácií, chybovosti pracovníka. Možné riziko: zvýšená odozva pre zákazníkov.

Oblasť dodávateľov

Zistené nedostatky a riziká v oblasti dodávateľov:

- Nedostatočná podpora pri technických problémoch. Možné riziko: výpadok systému.
- Veľmi zlou sa ukazuje podpora užívateľská, ktorej závislosť záleží od dostupnosti externého dodávateľa. Možné riziko: výpadok systému na celý deň.
- V podniku nie je uzavretá zmluva SLA s externým dodávateľom ERP systému a tak sa nemôže vyviesť objektívna zodpovednosť voči dodávateľovi. Možné riziko: finančné straty.

Oblasť managementu

Zistené nedostatky a riziká v oblasti managementu:

- Nízky záujem managementu o informačné systémy ako celku a významu pre podnik predstavuje priamu konkurenčnú nevýhodu. Možné riziko: zaostávanie voči konkurencii.
- Absencia informačnej stratégie vedie k neschopnosti merať celkovú efektivitu IS. Možné riziko: vysoké neriadené náklady.
- Nereflektovanie požiadaviek užívateľov IS môže viesť v konečnom dôsledku k používaniu zastaraného systému. Možné riziko: neefektivita práce, užívateľsky nepoužiteľný IS.

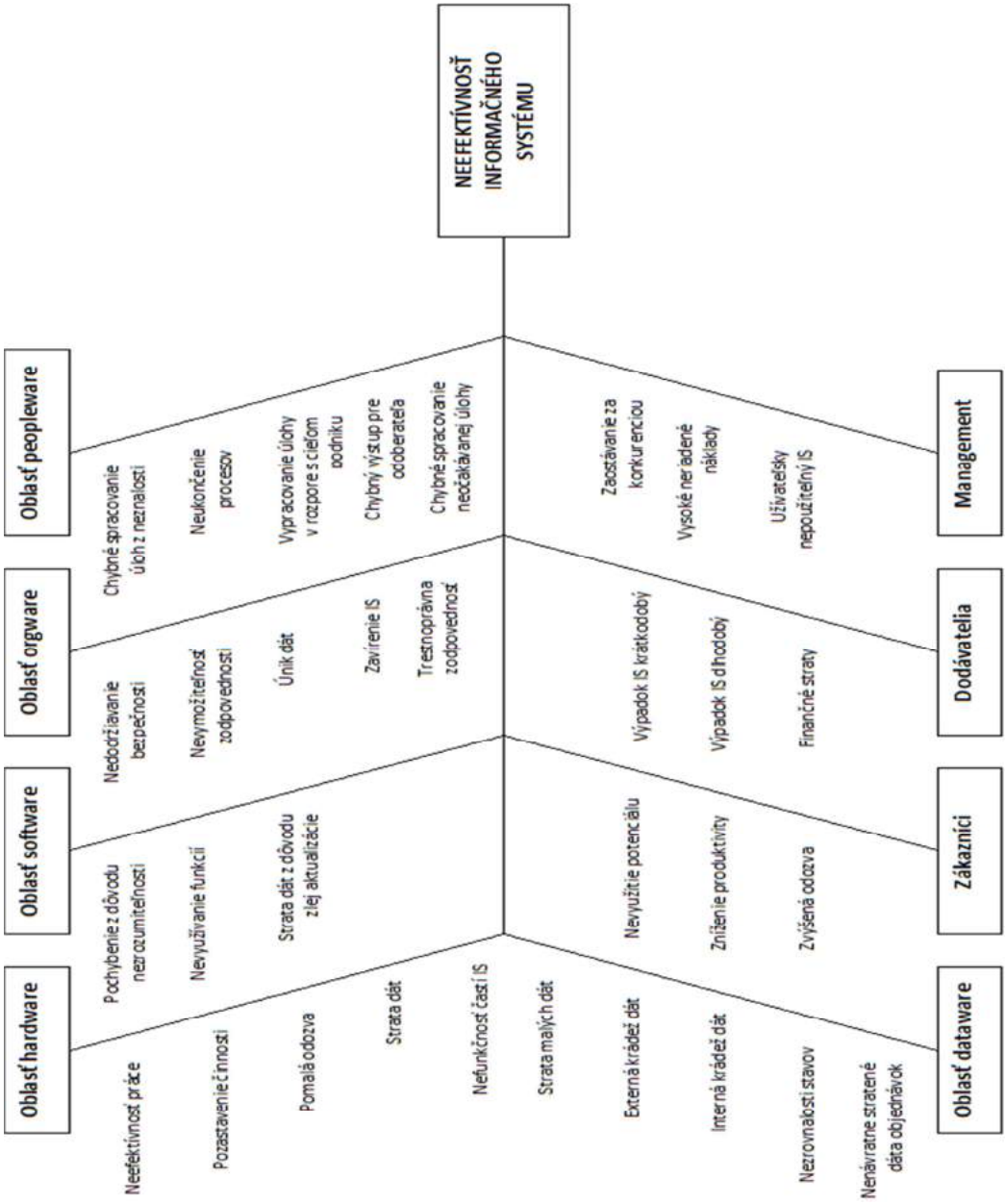
Oblasť informačnej bezpečnosti

Zistené nedostatky a riziká v oblasti informačnej bezpečnosti:

- Bezpečnostná politika nie je súčasť stratégie tak isto ako obmena hesiel. Nie sú zabezpečené zálohované dáta, nie sú zadefinované prístupy. Možné riziko : vniknutie do systému.
- Povedomie o bezpečnosti vo firme je minimálne a podnik nepracuje v súlade so systémom pre riadenie bezpečnosti informácií. Možné riziko: zrútenie systému.
- Chýbajúce smernice na definovanie metodiky zálohovania. Možné riziko: nedostatočné zálohovanie.

2.5.1 Ishikawa diagram

Rozborom informačného systému a dvoch dotazníkových metód boli nájdené riziká, ktoré môžu viesť k zníženiu efektívnosti informačného systému, prípadne až k jeho dočasnému zastaveniu. Riziká sú zobrazené Ishikawa diagramom, známym ako rybia kosť. Zobrazuje oblasti spôsobujúce neefektívnosť a ich príčiny (Tichý a Milík, 2006, s. 181). Nájdené riziká boli podľa ich charakteru rozdelené do kategórií, ktoré vychádzajú z oblasti metódy HOS 8.



Obrázok 13: Ishikawa diagram
(Zdroj: Vlastné spracovanie)

2.5.2 Vyhodnotenie rizík

Pre vyhodnotenie rizík bola zvolená kvantitatívna metóda podľa normy ČSN ISO/IEC 27005:2008. Ako vstup sú použité pravdepodobnosť výskytu scenára, od nepravdepodobnej až po veľmi vysokú, a dopad, od zanedbateľného až po veľmi vážny. Významnosť rizika je vyjadrená ako súčet pravdepodobnosti a jeho dopadu. Na vyhodnotenie je použitá stupnica rozdelená do troch častí: nízka významnosť predstavuje na podnik alebo financie zanedbateľný dopad, zvýšená predstavuje znateľný dopad na prevádzku podniku a vysoká významnosť predstavuje veľký nepriaznivý dopad najmä v oblasti financií (Smejkal a Rais, s. 134 a 135,2013).

Tabuľka 12: Pravdepodobnosť výskytu rizika

Pravdepodobnosť výskytu rizika	Slovné vyjadrenie	Hodnotenie
nepravdepodobná (0 % - 5%)	Riziko je nepravdepodobné, zanedbateľné.	1
nízka (5 % - 20 %)	Riziko je málo pravdepodobné.	2
stredná (20 % - 50 %)	Riziko je pravdepodobné, príležitostne.	3
vysoká (50 % - 70%)	Riziko sa objavuje často.	4
veľmi vysoká (70 % - 100 %)	Riziko sa objavuje veľmi často.	5

(Zdroj: Vlastné spracovanie podľa Rais a Smejkal, 2013)

Tabuľka 13: Význam rizika

Dopad	Slovné vyjadrenie	Hodnotenie
nevýznamný	Výskyt rizika neovplyvňuje prevádzku IS.	1
malý	Výskyt rizika je málo významný, nemá vážny, dlhodobý, finančný dopad	2
stredný	Výskyt rizika je významný, potreba riešenia nie je okamžitá.	3
vážny	Výskyt rizika je významný, potreba riešenia je naliehavá.	4
veľmi vážny	Výskyt rizika je pre podnik, alebo IS krízový.	5

(Zdroj: Vlastné spracovanie podľa Rais a Smejkal, 2013)

Tabuľka 14: Hodnotiaca tabuľka

Miera rizika		
2 - 4	nízka	Dopad na prevádzku IS je minimálny.
5 - 6	zvýšená	Dopad na prevádzku IS je zvýšený.
7 - 10	vysoká	Dopad na prevádzku IS je kritický.

(Zdroj: Vlastné spracovanie podľa Rais a Smejkal, 2013)

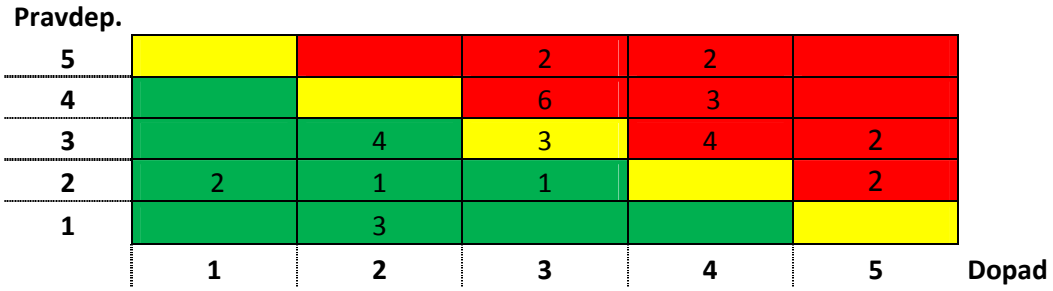
Nasledujúca tabuľka zobrazuje zistené rizika, ktoré sa môžu vyskytnúť u pozorovaného informačného systému. Významnosť je výsledkom súčtu pravdepodobnosti a dopadu.

Tabuľka 15: Vyhodnotenie rizík

Ozn.	Kategória	Riziko	Pravdep.	Dopad	Význ.
A	hardware	Neefektívnosť práce	1	2	3
B	hardware	Pozastavenie činnosti	2	5	7
C	hardware	Strata dát	4	3	7
D	hardware	Nefunkčnosť častí IS	1	2	3
E	software	Pochybenie z dôvodu nezrozumiteľnosti	2	1	3
F	software	Nevyužívanie funkcií	2	1	3
G	software	Strata dát z dôvodu zlej aktualizácie	2	3	5
H	orgware	Nedodržiavanie bezpečnosti	4	4	8
CH	orgware	Nevymožiteľnosť zodpovednosti	5	3	8
I	orgware	Únik dát	4	4	8
J	orgware	Zavírenie IS	5	4	9
K	orgware	Trestnoprávna zodpovednosť	3	5	8
L	peopleware	Chybné spracovanie úloh z neznalosti	4	3	7
M	peopleware	Neukončenie procesov	3	2	5
N	peopleware	Vypracovanie úlohy v rozpore s cieľom podniku	3	4	7
O	peopleware	Chybný výstup pre odoberateľa	3	2	5
P	peopleware	Vystavenie chybnej faktúry	3	3	6
R	peopleware	Chybné spracovanie neočakávanej úloh	3	2	5
S	dataware	Strata nezálohovaných malých dát	3	3	6
T	dataware	Externá krádež dát	5	4	9
Q	dataware	Interná krádež dát	3	5	8
U	dataware	Nenávratne stratené dáta objednávok	3	4	7
V	dataware	Nezrovnalosti stavov	4	3	7
W	zákazníci	Nevyužitie potenciálu IS	3	2	5
Y	zákazníci	Zníženie produktivity	2	2	4
Z	zákazníci	Zvýšená odozva smerom k zákazníkom	4	3	7
AA	dodávatelia	Výpadok systému krátkodobý	3	4	7
AB	dodávatelia	Výpadok systému dlhodobý	2	5	7
AC	dodávatelia	Finančné straty	1	2	3
AD	management	Zaostávanie za konkurenciou	3	4	7
AE	management	Vysoké neriadené náklady	4	3	7
AF	management	Užívateľsky nepoužiteľný IS	3	3	6
AG	bezpečnosť IS	Vniknutie do systému	4	3	7
AH	bezpečnosť IS	Zrútenie systému	5	3	8
ACH	bezpečnosť IS	Nedostatočné zálohovanie	4	4	8

(Zdroj: Vlastné spracovanie)

V nasledujúcom grafe je znázornená súčtová matica rizík. Zelenou je znázornená nízka významnosť rizika, žltou farbou zvýšená významnosť rizika, ktorá je v niektorých prípadoch akceptovateľná a červená predstavuje vysokú významnosť rizika, ktoré je neprijateľné a je potrebné ho riešiť čo najrýchlejšie.



Obrázok 14: Súčtová matica rizík
(Zdroj: Vlastné spracovanie)

V nasledujúcej časti budú návrhy riešení pre zlepšenie momentálneho stavu vedúcim k eliminácií rizík a hlavne ich príčin, ktoré ich spôsobujú. Bude sa jednať hlavne o riziká vyskytujúce sa v červenej oblasti a riziká s významnosťou 7 – 10 (viď tabuľka). Ako synergický efekt je očakávané zlepšenie aj ostatných rizík.

3. Návrh riešenia

3.1 Návrhy opatrení

V predchádzajúcej časti bola uskutočnená analýza súčasného stavu informačného systému, ktorý firma využíva. Na základe vykonanej analýzy boli zistené nedostatky, ktoré sa bude táto časť práce snažiť pomocou navrhnutých opatrení na zlepšenie vyriešiť a následne reflektovať ich prínosy.

Pomocou analýz HOS 8 a systémom zefis boli zistené nedostatky ovplyvňujúce vyváženosť a efektívnosť IS a následne hrozby, z ktorých vzišli riziká. Najviac problematické sa ukázali oblasti dodávateľov, orgware a dataware, ktorých nedostatky sa prejavujú aj v ostatných častiach IS. Pre jednotlivé oblasti boli navrhnuté nasledujúce opatrenia.

3.1.1 Oblasť orgware

Veľká časť možných hrozieb vyplýva z neexistujúcich pracovných postupov a smerníc a nezadefinovanej bezpečnostnej stratégie. Neexistuje tak záväzný predpis riešení vzniknutých situácií, ktorý by sa mohol dodržiavať a riadiť týmito zásadami, a ktorý by umožňoval postihy v opačných prípadoch.

Smernica by mala obsahovať pravidlá pre bezpečnosť a používanie IS:

- aké zariadenia je ktorý pracovník oprávnený využívať,
- finančná zodpovednosť za zverený majetok,
- zákaz inštalácie programov,
- zákaz pripájania vlastného hardware,
- určiť osobu, ktorá môže na požiadanie poskytnúť potrebný SW,
- poruchy HW a SW nahlasovať zodpovednej osobe,
- každý užívateľ bude mať pridelený vlastný účet,
- určenie zodpovednosti za vkladané dáta,
- obmedzenie používania prostriedkov k inej ako pracovnej činnosti,
- spôsob vykonávania záloh,
- prístupové heslá musia mať požadovaný počet znakov, zložitosť a byť menené v pravidelných intervaloch,

- zákaz vynášania firemných dát,
- postupy pri odchode z pracoviska.

Záverečné ustanovenia budú definovať osoby, ktoré sú oprávnené kontrolovať dodržiavanie smernice, aké postihy budú vyplývať z jej nedodržiavania a spôsob úhrady škôd pri jej nedodržiavaní.

Implementácia postupov by nemala predstavovať zvýšenie nákladov, ale len zadefinovanie pravidiel, aby bol v podniku priadok. Prístupové obmedzenia k dátam, ich zdieľanie a prípadné pripájanie HW súčastí zadefinuje zodpovedná osoba v nastaveniach operačného systému pod svojim administrátorským účtom v súlade so smernicou. Prístup do internetu potrebujú len dva útvary, z toho sa počítajú po jednom pracovníkovi. Navrhovaná podoba prístupu na internet, by mala byť zo samostatného PC, ktorý nie je súčasťou IS.

Spolu so smernicou je potrebné zadefinovať informačnú stratégiu, ktorá obsahuje ciele a hlavné vlastnosti budúceho stavu a vývoja. Informačná stratégia je dôležitá z pohľadu podnikovej stratégie a jej zmysel je v naplňovaní cieľov podniku ako celku. Na jej tvorbe by sa mali názorovo účastniť všetci zamestnanci, tak, aby vznikla komplexná informačná štruktúra.

Ciele informačnej stratégie:

- Neustále zlepšovanie podnikového informačného systému.
- Udržiavanie hw a sw vybavenia na požadovanej úrovni.
- Poskytovanie všetkých funkcií, potrebných pre prácu užívateľov.
- Poskytovanie informácií k zvyšovaniu produktivity.
- Podpora jednotlivých procesov podniku.
- Definovanie bezpečnostnej politiky.
- Návratnosť vložených prostriedkov.
- Školenia v oblasti IS.
- Pravidelná analýza využívaných aplikácií.

Vzhľadom k nedostatkom ohľadne bezpečnosti a používania IS je potrebné uviesť bezpečnostné smernice do platnosti školeniami, ktoré zabezpečí zodpovedná osoba.

Školenie by malo byť zamerané na bezpečnosť informácií, kde budú užívatelia oboznámení s jednotlivými prvkami informačnej bezpečnosti. Budú tak poučení o jej dôležitosti a pravidlách bezpečného užívania. Tu aj podpíšu dodatok k pracovnej zmluve, aby pravidlá boli vymáhateľné. Každý nový zamestnanec bude následne školenie absolvovať osobitne.

Druhý typ školenia by mal byť zameraný primárne na ovládanie informačného systému. Tohto školenia by sa mal zúčastniť každý užívateľ. Jeho účelom by malo byť zoznámenie sa s prostredím a ukážky práce v ňom. Tiež by poskytoval priestor na zodpovedanie otázok ohľadom užívania. Užívateľom by bolo názorne zobrazené, ktoré funkcie pri svojej práci potrebujú a ako ich využívať. Toto školenie by zabezpečoval externý pracovník, raz ročne, prípadne pri významných aktualizáciách systému. Užívatelia si tu aj zopakujú užívanie funkcií, ktoré nevyužívajú denne.

3.1.2 Oblasť dodávateľov

Táto oblasť trpí nedostatkami hlavne v prípade vzniku problémov. Technickú podporu si momentálne podnik zaisťuje svojpomocne, konateľom spoločnosti, ktorý nie je vždy k dispozícii a nemá absolútnu technickú znalosť k riešeniu každého problému. Navrhovaným riešením je zavedenie úseku IT, ktoré by obsiahol jeden pracovník ako správca sietí. Ten by bol v podniku pripravený riešiť všetku technickú podporu v prípade potreby, reakčný čas by sa tak znížil na menej než pár minút. Jeho pracovnou náplňou by sa, mimo iné, stala príprava systému na zavedenie internetového obchodu.

Užívateľská podpora sa týka najmä pomoci so systémom v prípade vzniku problému. Väčšina vzniknutých situácií sa po novom bude dať riešiť vďaka zodpovednému pracovníkovi, ktorý môže kontaktovať dodávateľa systému e-mailom, alebo telefonicky. V prípade potreby by dodávateľ služby vyslal svojho technika. Je potrebné, aby sa zrealizovala s dodávateľom zmluva, ktorá zabezpečí, že doba odozvy na požiadavku bude maximálne 2 hodiny a doba vyriešenia najneskôr do 24 hodín. Dodávateľ sídli v rovnakom meste ako analyzovaný podnik, preto by nemala byť požiadavka nezrealizovateľná.

3.1.3 Oblasť hardware

Táto oblasť vykazuje relatívne dobrú úroveň, technické vybavenie je dostačujúce a systémy nemajú veľkú odozvu. Výnimkou však boli stanice na predajni, kde 2 počítače boli výrazne zastarané a prácu predavačom merateľne spomaľovali. Na tieto dve pracovné stanie sa preto odporúča zakúpiť nové koncové zariadenia. Podľa požiadaviek na bezproblémový chod modulu Money Kasa Professional:

Tabuľka 16: Požiadavky na modul

HP Pro 285 G2 MicroTower	
Procesor	AMD 3,6 GHz
Pamäť	4 GB RAM
Kapacita	500 Gb

(Zdroj: Vlastné spracovanie podľa money.cz)

Prvok automatizácie by mohli do procesov zaviesť čiarové kódy. Týmto spôsobom sa zaktualizuje spôsob zadávania dát do IS a jeho samotné využívanie. Aby bol tento plán úspešný sú potrebné niektoré predpoklady, ktoré už v podniku sú. Je to nedostatočne využívaný systém Money, ktorý je ready-made na pripojenie čítacieho zariadenia a skladové karty bez priradených čiarových kódov. Prepojenie zariadenia a IS predĺži zamestnancovi klávesnicu priamo do ruky. Informácie sa budú spracovávať v reálnom čase, čo umožní zber a kontrolu informácií v momente uskutočnenia úkonu. Po zavedení by sa v sklade mali prestať využívať papierové objednávky prijaté od nákupcov, čím sa odstráni papierová dokumentácia ako nosič informácií, ktorý sa doteraz musí prenášať medzi jednotlivými úsekmi, kontrolovať a následne prepisovať údaje do systému.

Na bezproblémové prúdenie informácií je potrebné pokryť sklad bezdrôtovou sieťou, čo nie je problém v prípade skladu, ktorý je v tomto prípade otvorený priestor. Na zabezpečenie kontaktu sa na sklad zaobstará acces point - bezdrôtový hub s bezdrôtovým modulom, prostredníctvom ktorého budú skenery komunikovať na diaľku. Pre prípad SW sa využije zabehnutý systém Money. V rámci inštalácie sa nebude využívať nový terminál s vlastným OS a ďalšou aplikáciou. Výber konkrétneho skeneru bol uskutočnený tak, aby prežil záťaž v prašnom prostredí a iné mechanické vplyvy a obsahoval klávesnicu so znakovým displayom. Výdrž akumulátorov by mala byť nastavená tak, aby vydržali celý pracovný deň. Odporúčajú sa priemyselné skenery

najvyššej triedy, u ktorých je predpoklad menšej poruchovosti a technologického zastarania.

Sklad je plne elektrifikovaný a na pracovných staniciach sa nachádzajú počítače napojené na lokálnu sieť. Šíriť signál bude acess point napojený na sieť, ktorá je vedená do centrálneho ethernet a smerovať odtiaľ do existujúceho servera s aplikáciou. Výkon acess pointu je prenosová rýchlosť 54 Mbps na frekvencii 2,4Ghz a protokole IEEE 802.11g, čo zaručí kompatibilitu s terminálmi. Čiarové kódy sa budú tlačiť na stacionárnej tlačiarni samolepiacich štítkov, ktorá bude umiestnená na novom pracovisku IT.

Nakupovanie nového vybavenia bude mať na starosti nový pracovník a tak by sa malo k nákupom pristupovať s vyváženosťou a kompatibilitou k existujúcim komponentom.

3.1.4 Oblasť software

Aktuálna situácia nevyžaduje radikálne zmeny informačného systému vo firme. Podnik je spokojný s existujúcim softwerom, do budúcna sa plánuje s rozšírením o niektoré moduly, ktoré ma spoločnosť Money v ponuke.

Pri skúmaní možností bolo zistené že nákupcovia nemajú v položkách sklad zadefinované jednotlivé zľavy pre odoberateľov, čo znižuje ich nahraditeľnosť v prípadoch výpadku. Toto sa po úspešnom preškolení spolu s nový zamestnancom vyrieši, a tak v prípade nedostupností nákupcov budú ovládať cenové relácie aj ostatní zamestnanci a v prípade potreby budú vedieť poskytnúť informácie, ktoré nemali k dispozícii. Nainštaluje sa aj nové rozšírenie, ktoré bude informovať a upozorňovať o dodávke tovaru.

V prípade chybových hlásení a nastaní neočakávaných udalostí je k dispozícií technik a malo by sa tak zabrániť pochybeniam z dôvodu nezrozumiteľnosti. Na technika sa podnik môže spoliehať aj v prípade nových aktualizácií systému, ktoré nie vždy prebehli bezproblémovo a firma bola odkázaná na externého pracovníka.

3.1.5 Oblasť peopleware

S predošlými návrhmi sa automaticky znižujú niektoré sprievodné riziká v ostatných oblastiach, ako napríklad peopleware. So zabezpečenými školeniami by sa mali

eliminovať chybné spracovania faktúr, predajov a zmien pohybov na sklade. Využitie modulu sklad so všetkými jeho funkciami ako sú cenové kategórie jednotlivých odoberateľov zvýši zastupiteľnosť pracovníkov na nákupe a predaji. Na zvýšenie zastupiteľnosti sa zvolí zástupca hlavného nákupcu a predajcu, ktorý sa doškolí na úroveň potrebnú v prípade, že títo nie sú na pracovisku a zvýši sa tak zastupiteľnosť týchto dvoch kľúčových pozícií. Správca sietí môže vykonávať kontrolu uskutočnených obchodov a zamestnanci nemôžu svojvoľne udeľovať zľavy. Toto riziko sa eliminuje aj nastavením právomocí na pracovnej stanici pokladňa. Čítacie zariadenie odbremení zamestnancov od manuálneho vkladania položiek do systému, keďže tie sa budú po nascanovaní hromadiť v rade na spracovanie priamo v IS, čím sa eliminujú možné chyby pri výstupoch v rámci dokladov.

3.1.6 Oblasť dataware

Veľké dáta z obchodu a účtovníctva sa každý deň zálohujú - je potrebné aby sa zálohy každý deň uzamykali do trezoru a boli chránené pred krádežou. Malé dáta, za ktoré považujeme údaje z jednotlivých staníc, hlavne z balíka MS Office sa však nezálohujú takmer vôbec. Ako ideálne riešenie sa ponúka služba balíka MS Office 365 bussines, ktorá ponúka cloudove riešenie v podobe úložiska OneDrive. Tá umožňuje vytvorenie zložky, ktorá je synchronizovaná s úložiskom. Odporúča sa tak zakúpiť tento balík na 4 pracovné stanice pre nákup a predaj. Dáta z MS Office budú zálohované a v prípade potreby aj dostupné z iného PC. Manuálne spracovanie objednávok spôsobovalo v niektorých prípadoch stratu papierového nosiča informácií; to už by sa nemalo vyskytovať. Vďaka čítačkám čiarových kódov je očakávaný aj väčší súlad stavov pri vykonávaní inventúry.

Nový pracovník v súlade so smernicami zreguluje prístupy jednotlivých staníc do vonkajšieho prostredia. Zablokovanie portov na pridávanie externých zariadení zabráni možnosti pripojiť externé zariadenia a krádeži dát. Voči hrozbám z vonkajšieho prostredia je IS zabezpečený prvkami ako sú antivirus, firewall a anti-spyware.

3.1.7 Oblasť zákazníci

V oblasti zákazníkov je potrebné uskutočniť niektoré zmeny, ktoré povedú k zlepšeniu stavu. Zákazníci získajú rýchlejšiu odozvu vďaka zakúpenému HW. V súčasnosti nie sú definované ciele informačného systému, tie sa zadefinovali v oblasti orgware.

Následne by bolo vhodné zadefinovať určité metriky, ktoré by umožňovali sledovanie plnenia cieľov, fungovanie IS a iné. V súčasnej dobe nie sú známe ani očakávania užívateľov od systému.

Aby bolo možné priebežne hodnotiť informačný systém, je potrebné stanoviť jeho metriky, na základe ktorých bude možné zistiť, či systém plní požadované ciele a či funguje podľa potrieb vedenia spoločnosti a samotných užívateľov. Voľba metrík je individuálna. Pre potreby sledovaného podniku boli navrhnuté metriky uvedené v nasledujúcej tabuľke.

Tabuľka 17: Metriky informačného systému

Metrika	Popis	Jednotky
Dostupnosť informačného systému	Plánovaná dostupnosť dostupnosť / výpadky	95%
Spokojnosť užívateľov s informačným systémom	Spokojnosť zisťovaná pomocou dotazníkov	90%
Počet výpadkov informačného systému	Počet všetkých incidentov za mesiac	3
Rýchlosť odozvy podpory na požiadavky	Maximálna akceptovaná doba od nahlásenia požiadavku a reakcia	1 hodina
Rýchlosť vyriešenia technickej požiadavky	Maximálna doba od nahlásenia po vyriešenie	3 hodiny
Rýchlosť vyriešenia užívateľskej požiadavky	Maximálna doba od nahlásenia po vyriešenie	8 hodín (pracovný deň)

(Zdroj: Vlastné spracovanie)

Informačný systém je nutné priebežne sledovať a zrovnávať zistené hodnoty so stanovenými metrikami a reagovať na požiadavky jeho užívateľov. V prípade, že informačný systém napĺňa hodnoty metrík, dá sa považovať jeho stav za uspokojivý. V opačnom prípade je potrebné situáciu riešiť a to buď so správcom sietí, alebo s externým dodávateľom.

3.1.8 Oblasť managementu

Nízky záujem managementu, resp. vedenia spoločnosti, o oblasť informačných systémov môže viesť postupom času k zaostávaniu oproti konkurencii, preto je potrebné, aby sa zúčastnilo školení aj vedenie firmy a bralo do úvahy spätnú väzbu zamestnancov užívajúcich systém. Vytvorením informačnej stratégie, smernice

o prevádzke a zavedení metrík by malo byť možné sledovať aj náklady na prevádzku systému.

3.1.9 Oblasť informačnej bezpečnosti

Navrhnutá bezpečnostná politika by mala zabezpečovať zaistenie dostupnosti, vierohodnosti a integrity informácií poskytovaných informačným systémom. Analýza zistila, že nie je najväčšou starosťou fyzická ochrana technológii, ale zlyhanie jednotlivých zamestnancov v prípadoch neznalosti, nedbalosti, alebo úmyselného poškodenia podniku. Okrem chýb softwaru, krádeží, technických porúch, má každý zamestnanec individuálnu zodpovednosť k informačnému systému, s ktorým pracuje. Z analýzy bezpečnosti informačného systému vyplýva, že pokiaľ nebude zavedené riadenie a správa informačnej bezpečnosti, nemôžu mať spoľahlivú účinnosť kroky zavedené na technickej úrovni, ako napríklad zálohy dát, heslá, antivírusové zabezpečenie. Bezpečnostná politika k naplneniu svojho účelu by mala byť:

- spracovaná v písomnej forme,
- záväzná pre všetkých v podniku,
- v povedomí každého, koho sa týka,
- byť vymáhateľná,
- vôľa z managementu na jej tvorbe.

Školenie v oblasti informačnej bezpečnosti

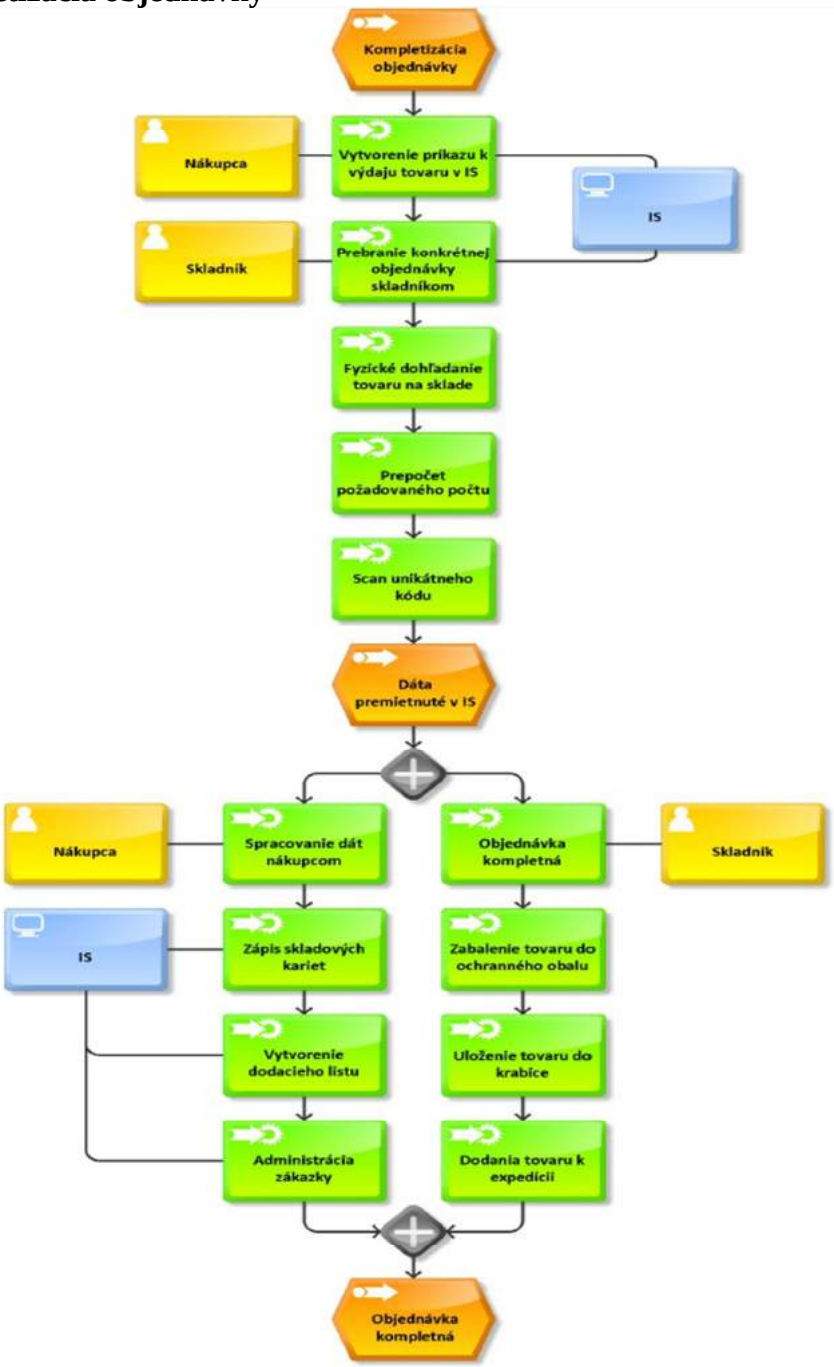
Cieľom školenia by malo byť oboznámiť sa s problematikou informačnej bezpečnosti a metódami riadenia bezpečnosti, a poskytnúť návod tak, aby sa stala každodennou súčasťou podniku. Jeho štruktúra je nasledovná:

- úvod do informačnej bezpečnosti,
- hrozby informačnej bezpečnosti:
    - vnútorné, vonkajšie hrozby,
    - nebezpečenstvo elektronickej komunikácie,
    - aktuálne hrozby z internetu,
- metódy riadenia informačnej bezpečnosti,
- pravidlá pre užívateľov
- zhrnutie.

3.2 Zvýšenie efektívnosti

Aby bolo možné dopracovať sa k merateľným prínosom riešení, ktorých úžitky sú hodnotené subjektívne, nepriamo a ťažko identifikovateľné pokiaľ v skutočnosti nenastanú, boli vybrané konkrétne procesy obchodnej činnosti, na ktorých dopad návrhov je možno pozorovať okamžite.

Kompletizácia objednávky



Obrázok 15: Procesná mapa kompletizácie objednávky
(Zdroj: Vlastné spracovanie)

Na pokyn od nákupcu z oddelenia sa začne spracovávať objednávka, skladník začne plniť úlohu nasledovne: pohybuje sa k pozíciám tovaru, ktorý je vyžadovaný a zoberie do ruky určený počet kusov položky a nascanuje priradený kód. Počet kusov potvrdí na klávesnici. Súbežne prebieha aj kontrola správnosti, ktorá sa predtým vykonávala na baliacej stanici. V prípade pochybenia sa upraví zadaný počet na klávesnici na mieste. V tom istom čase sú už dáta v informačnom systéme na stredisku predaj, kde sa nascanované položky v systéme Money pridávajú do rady, pripravené na spracovanie formou faktúry alebo dodacieho listu.

Celý proces sa citeľne urýchli vďaka odstráneniu pohybov navyše, od pozícií tovarov na pôvodnú vychystávaciu stanicu, ktorý by bol ušetrený od vyškrtávania nachystaného tovaru na papieri, odpadne aj ručné vyhľadávanie tovaru v PC, v prípade jeho nenájdenia. Optimalizácia objednávania umožní súbežne vytváranie dodacieho listu predajcovi a nemusí tak ručne upravovať skladové karty a tvoriť dokumenty pre odoberateľa.

Tabuľka 18: Predpokladaná doba činnosti po zavedení návrhov

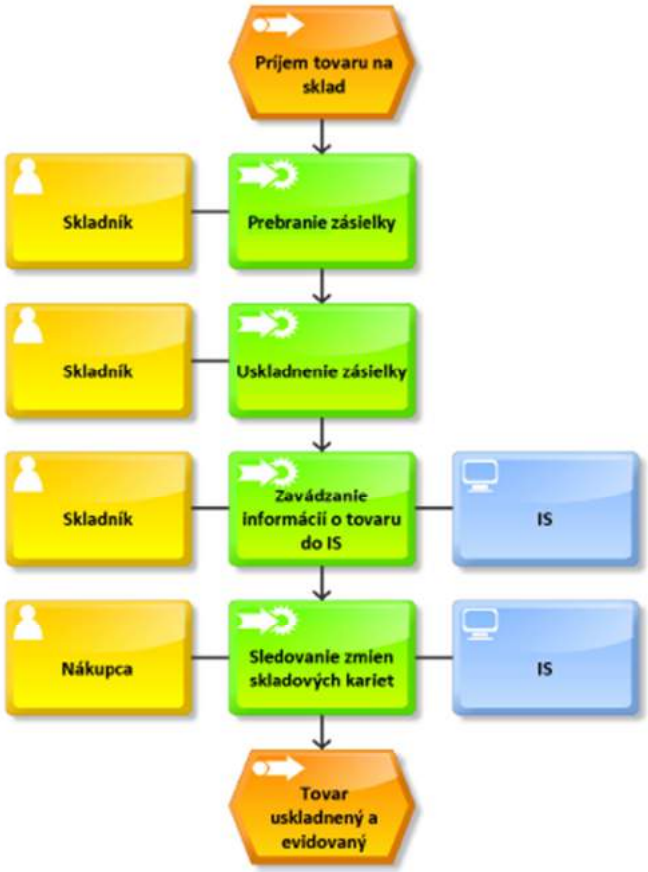
Činnosť	Čas činnosti pred (s)	Čas činnosti po (s)
Doručenie objednávky na sklad	20	20
Chôdza od stanice k regálom	75	75
Vyhľadanie požadovaných tovarov	600	540
Kontrola pripraveného obsahu	120	~~0~~
Odovzdanie objednávky nákupcovi	20	~~0~~
Tvorba faktúry a dodacieho listu	360	120
Zabalenie a zalepenie balíku	45	45
Nalepenie etikety	10	10
Presun na paletu	20	20
Celkom	1270	830

(Zdroj: Vlastné spracovanie)

Pri porovnaní je vidieť, že priemerný čas potrebný na kompletizáciu objednávky sa znížil o 440s.

Prijatie tovaru na sklad

Výstupom od nákupcu z administratívneho pracoviska sa stane skladový rozkaz, ktorý bude čakať na realizáciu. Po tom ako skladník príjme tovar od dodávateľa a po kontrole dodaného množstva s dodacím listom, sa ukladaný na svoje pozície súčasne sníma kód položky a pomocou klávesnice zadáva počet kusov, následne potvrdí zaradenie tovaru, v tomto momente prichádza k zaneseniu informácie do IS prostredníctvom skeneru. Nákupcovi na pozadí prebieha úprava skladovej karty, po skončení procesu príjmu na sklad aktualizáciu potvrdí. V prípade rozdielnych cien údaj zmení. Nákupca už nemusí ručne opisovať dodací list a vyhľadávať skladové karty. Odhadnutý ušetrený čas je 660s. Ak pôjde o nový tovar, vytvorí sa nová skladová karta, priradí pozícia a na tlačiarni sa vytlačí čiarový ód s informáciou.



Obrázok 16: Procesná mapa prijatia tovaru
(Zdroj: Vlastné spracovanie)

Spracovanie objednávky

Jednotlivé časti spracovania objednávky, sa vďaka lepšej konfigurácií systému Money zautomatizovali tak, že nákupca nie je jediný kto vie, prípadne má poznačené, ktorý odoberateľ má aké cenové hladiny, a tak sa odstránila potreba kalkulovania ceny

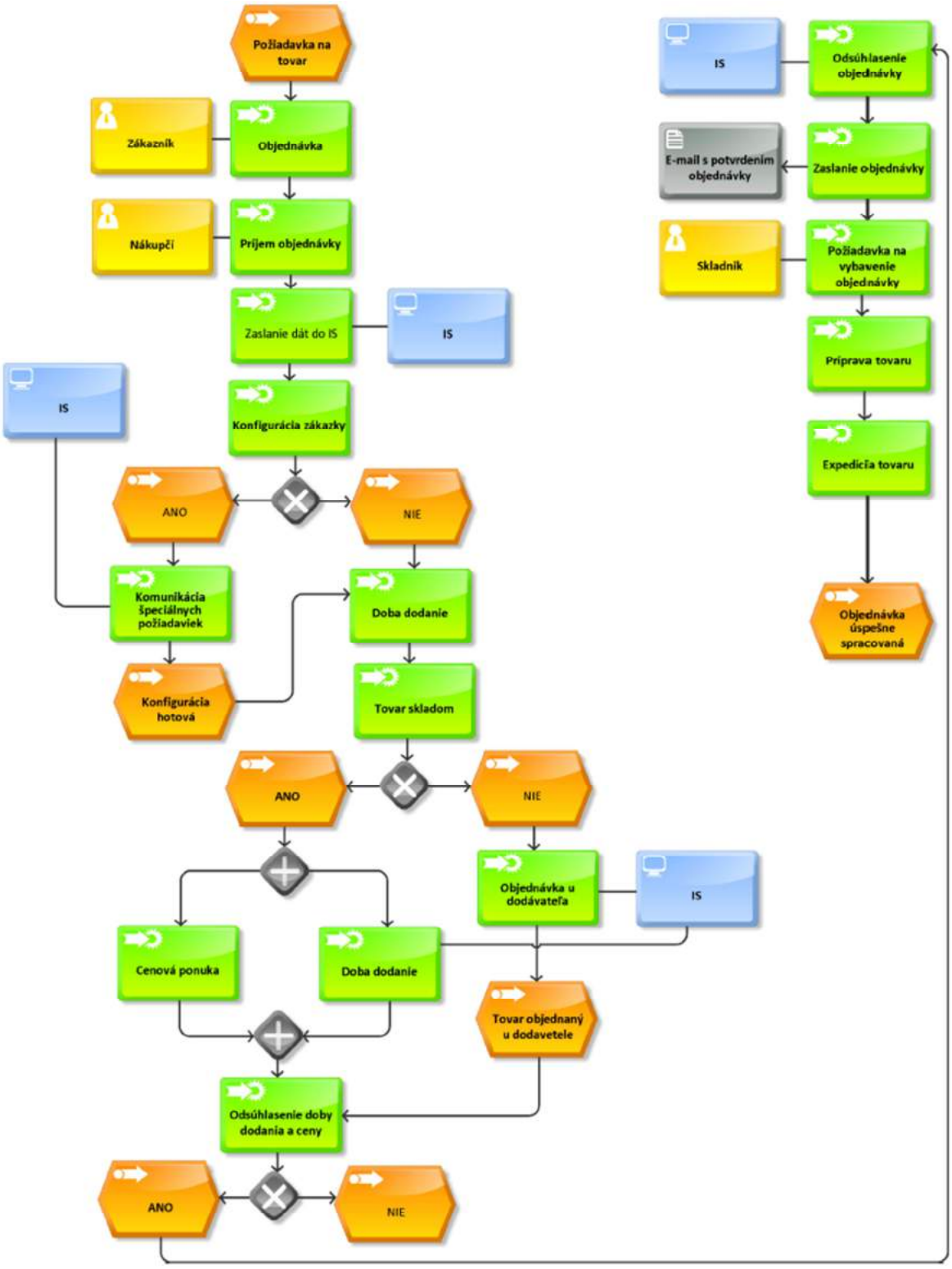
pri bežnej objednávke. Taktiež už nie je potreba, aby zisťoval stav skladu a čas dodania. V plánovanej konfigurácií systému sa ráta s automatizovaným systémom objednávok. Jednotlivé moduly sa nastavia tak, aby bola v IS zavedená automatická diferenciácia cien pre odoberateľa, závislá na objeme obchodných vzťahov, resp. dĺžky spolupráce. Cenníky sú aktuálne natavené na celý sortiment rovnakou úrovňou zľavy pre konkrétneho partnera, čo je postačujúce iba pre maloobchod. V rámci veľkoobchodu musia byť hladiny zliav aj v jednotlivých skupinách tovarov. Na správne vedený sklad je potrebné, aby sa vedelo čo skladom je a kedy má aký tovar prísť. Na základe skenerov by mali existovať úplné a aktuálne informácie o fyzických zásobách. Rozšírenie podlimitnej zásoby vie generovať objednávky, resp. upozorňovať na nízke stavy. Odoberateľ, ktorý si objedná tovar, dostáva ihneď odpoveď prakticky od ktoréhokoľvek pracovníka, ktorý zdvihne telefón, alebo číta e-mail. Ak si náhodou objednáva tovar, ktorý nie je skladom, systém sám automaticky zobrazí, kedy bude opäť žiadaný tovar skladom. Takýmto spôsobom bude odpoveď na dopyt spracovaná rýchlejšie a predíde sa častým doplňujúcim otázkam od zákazníka na potvrdenie dodacieho termínu a ceny. Tieto rozhovory bývajú súčasne viackolové, kedy sa po zložení telefónu, prípadne odpovedi na prvý mail, zisťujú ďalšie údaje. Návrhom by sa predišlo potrebe predajcu pri každom dopyte, kým sa objednávka vloží do IS.

Tabuľka 19: Predpokladaná doba činností po zavedení návrhov

Činnosť	Čas činnosti pred (s)	Pridaná hodnota
Príjem objednávky	5	5
Kalkulácia cien	120	10
Výpočet dodacej lehoty	45	10
Celková komunikácia so zákazníkom	330	200
Vytvorenie objednávky v IS	125	100
Celkom	625	325

(Zdroj: Vlastné spracovanie)

Priemerná dĺžka spracovania objednávky sa skrátila o 300s, kedy pracovníci nemusia zisťovať informácie a koordinovať ich s ostatnými pracovníkmi.



Obrázok 17: Procesná mapa spracovanie objednávky
(Zdroj: Vlastné spracovanie)

3.3 Vplyv navrhnutých opatrení na identifikované riziká

Vďaka zavedeným jednoznačným bezpečnostným pravidlám a smernici v oblasti používania IS a zadefinovaní stratégie, sa znížili pravdepodobnosti vysokého výskytu rizík na úroveň neohrozujúcu podnik. Na základe navrhnutých metrík sa odporúča

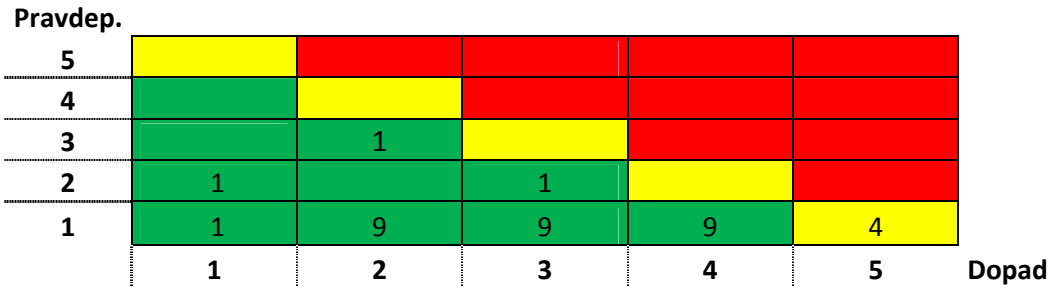
sledovať, či dochádza k dodržiavaniu pravidiel. Každý zamestnanec bude mať prístup k informáciám, ktoré potrebuje k svojej práci. Bude zabránené svojvoľnej manipulácií s údajmi a budú obmedzené prístupy smerom mimo podnik. Pracovníci po zavedení návrhov nebudú môcť nijakým spôsobom potenciálne odnášať dáta z podniku. Ich ochrana je vyriešená svedomitým spôsobom zálohovania a na vzniknuté technické problémy bude dohliadať určený pracovník. Automatizácia vďaka skenerom priniesla do systému jeho zrýchlenie na požiadavky a zamedzila chybným spracovaniam úloh.

Tabuľka 20: Hodnotenie rizík po zavedení opatrení

Ozn.	Kategória	Riziko	Pravdep.	Dopad	Význ.
B	hardware	Pozastavenie činnosti	1	5	6
C	hardware	Strata dát	1	3	4
E	software	Pochybenie z dôvodu nezrozumiteľnosti	1	1	2
H	orgware	Nedodržiavanie bezpečnosti	1	4	5
CH	orgware	Nevymožiteľnosť zodpovednosti	1	3	4
I	orgware	Únik dát	1	4	5
J	orgware	Zavírenie IS	1	4	5
K	orgware	Trestnoprávna zodpovednosť	1	5	6
L	peopleware	Chybné spracovanie úloh z neznalosti	1	3	4
M	peopleware	Neukončenie procesov	2	2	4
N	peopleware	Vypracovanie úlohy v rozpore s cieľom podniku	1	4	5
O	peopleware	Chybný výstup pre odoberateľa	1	2	3
P	peopleware	Vystavenie chybnej faktúry	1	3	4
R	peopleware	Chybné spracovanie neočakávanej úloh	1	2	3
S	dataware	Strata nezálohovaných malých dát	1	3	4
T	dataware	Externá krádež dát	1	4	5
Q	dataware	Interná krádež dát	1	5	6
U	dataware	Nenávratne stratené dáta objednávok	1	4	5
V	dataware	Nezrovnalosti stavov	2	3	5
Y	zákazníci	Zníženie produktivity	1	2	3
Z	zákazníci	Zvýšená odozva smerom k zákazníkom	1	3	4
AA	dodávatelia	Výpadok systému krátkodobý	1	4	5
AB	dodávatelia	Výpadok systému dlhodobý	1	5	6
AD	management	Zaostávanie za konkurenciou	1	4	5
AE	management	Vysoké neriadené náklady	1	3	4
AF	management	Užívateľsky nepoužiteľný IS	1	3	4
AG	bezpečnosť IS	Vniknutie do systému	1	3	4
AH	bezpečnosť IS	Zrútenie systému	1	3	4
ACH	bezpečnosť IS	Nedostatočné zálohovanie	1	4	5

(Zdroj: Vlastné spracovanie)

V nasledujúcom grafe je súčtová matica všetkých rizík po zohľadnení návrhov. Úspešne sa eliminovali riziká, ktoré mali vysoký vplyv na informačný systém, na úroveň, ktorá je tolerovateľná. Návrhy mali vplyv na väčšinu rizík.



Obrázok 18: Súčtová matica po zavedení opatrení
(Zdroj: Vlastné spracovanie)

3.4 Náklady na navrhované opatrenia

Celkové náklady na navrhnuté opatrenia, vrátane dvoch celoročných platieb na výplatu nového zamestnanca a službu Office 365 sú 15 390 €. Výsledná čiastka je pre podnik prijateľná a neohrozí vážne jej mesačné príjmy. Z dôvodu zastaraného hardware vybavenia sa kúpili dva PC na pokladňu a jeden novému zamestnancovi. Ďalšími nákladmi v oblasti hardware sú čítačky čiarových kódov a potrebná architektúra k nim. Počíta sa s dvoma školeniami ročne k IS Money, tie by sa už nemali ďalšie roky opakovať, ich agendu preberie zamestnanec.

Tabuľka 21: Náklady

Položka	Počet	Cena celkom
Hardware		
HP Pro 285 G2 MicroTower	3 ks	588 €
Náklady na čítačky		
Datalogic powercan 8300DK	5 ks	4 000 €
Wifi AP Netgear WNDAP360	1 ks	200 €
stacionárna tlačiareň	1 ks	280 €
Software		
Office 365	1 ks	106 € / rok
Školenie Money	14 h	616 €
Personálne náklady		
Nový zamestnanec	1 ks	9600 € / rok
Celkom		**15 390 €**

(Zdroj: Vlastné spracovanie)

Hardware bol nacenený podľa ponuky dlhoročného dodávateľa zariadení, u ktorého má firma zľavu a porovnaný s internetovým obchodom www.alza.sk. Office 365 sa predáva ako licencia pre 5 počítačov, čo pre potreby podniku postačuje. Cena školenia vychádza podľa cenníka lokálneho dodávateľa služieb a cena na zamestnanca bola odhadnutá podľa priemernej výšky mzdy na obdobných pozíciách v regióne (cena je uvedená v hrubom). Využiteľnosť nového zamestnanca bude okrem pozície správca sietí taktiež zavádzať čiarové kódy - táto práca je odhadovaná na tri mesiace. Následne by podnik mohol využiť daného zamestnanca pri implementácii internetového obchodu. S ďalšími nákladmi, napríklad na údržbu, či podporu, sa v rozpočte nepočíta, z dôvodu, že tieto náklady sa dajú považovať za prevádzkové a nie je vopred jasné, koľko ich v priebehu roka bude podnik potrebovať.

Jedna z možností ako vypočítať návratnosť investície a zvážiť tak realizáciu zmienených investícií je statická metóda pomeru nákladov a prínosov z projektu, keďže vyhodnocovanie efektívnosti vložených financií do informačného systému je len ťažko kvantifikovateľné. Vychádzalo sa zo zmapovaných procesov, v ktorých je možné zachytiť zmenu.

Tabuľka 22: Celkový ušetrený čas

Proces	počet/deň	ušetrený čas
Kompletizácia objednávky	32	~ 4 hod
Spracovanie objednávky	23	1 hod 55 min
Príjem tovaru	2	2 hod 15 min
Celkom		**8 hod 10 min**

(Zdroj: Vlastné spracovanie)

V sklade sa skompletizuje v priemere 32 balíkov za deň, ktoré ušetria 4 hodiny. 23 objednávok je takých, ktorým administratívni pracovníci musia venovať maximálny nameraný čas, zvyšné sú od stálych odoberateľov, ktorí objednávku pošlú a nepotrebujú ďalšie špecifikácie. Príjem tovaru ušetrí spracovateľovi dodacieho listu 2 hodiny 15 minút. Spolu tak z meraných procesov vzišlo 8 hodín navyše pre pracovníkov. Dá sa tak uvažovať o jednom ušetrenom pracovnom mieste. V analyzovanom období sa podnik rozhodoval či nepríjme nového zamestnanca z dôvodu nedostačujúcich kapacít. Úspora takéhoto mzdového nákladu predstavuje 630 € mesačne, a teda 7560 € ročne. Návratnosť finančných prostriedkov by na základe vyššie uvedeného predpokladu bola 2 roky.

3.5 Prínosy návrhov riešení

Hlavným prínosom pre spoločnosť je vyváženie existujúceho informačného systému na optimálnu úroveň všetkých ôsmych základných oblastí podľa metódy HOS 8, čo je jedna z podmienok efektívnosti IS a následného zefektívnenia tohto systému. Prínosy sú spojené predovšetkým s organizáciou informačného systému. Vďaka zavedeniu a dodržiavaniu bezpečnostných smerníc sa zlepší stav a kompletné zabezpečenie informačného systému, znížia sa riziká strát, úniku alebo poškodenia dát.

Zavedenie školení predstavuje pre podnik výhody v podobe zlepšenia znalostí a využiteľnosti informačného systému a ochrany informácií. Užívatelia tak zrýchlia svoju činnosť a reakcie v neočakávaných situáciách, následne by malo byť vylúčené ohrozovanie bezpečnosti svojim správaním a v prípade nedodržiavania je možné využiť sankcie. Školenia v oblasti používania prinesie zlepšenie predovšetkým vo zvýšení efektivity práce s IS a spoločne celého informačného systému.

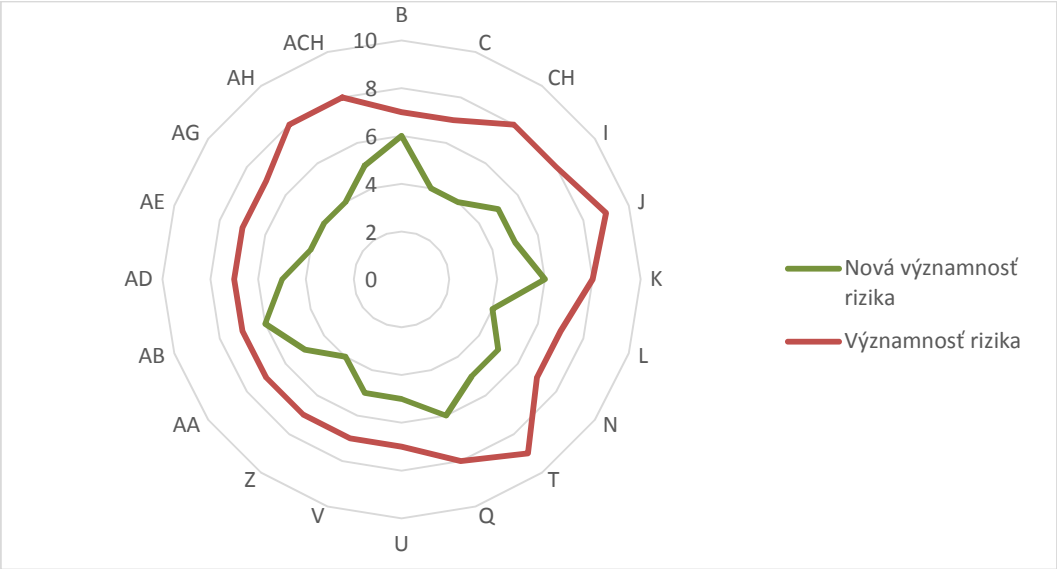
Navrhnuté opatrenia prinesú v oblasti peopleware a zákazníkov zefektívnenie využívaného systému. Očakávaná je znížená chybovosť a lepšie využívanie systémových funkcií. Vďaka opatreniam ako sú zadefinovanie cenových skupín pre odoberateľov a určenie zástupcov hlavných nákupcov a predajcov sa zvýši ich zastupiteľnosť. Správca sietí môže vykonávať kontrolu uskutočnených obchodov. Zavedením metrík informačného systému bude podnik sledovať priebežne jeho stav a plnenie cieľov, čo umožní reagovať včas na prípadné chyby a nedostatky, ktoré bude potrebné odstrániť.

Nový pracovník bude môcť poskytovať interné školenia, podieľať sa na tvorbe informačnej stratégie a dohliadať na jej dodržiavanie. Bude k dispozícii ako technická podpora a zamestnanci sa na neho budú môcť obrátiť aj v prípade užívateľských problémov. Vďaka správcovi sietí, nebude potrebné využívať služby externého pracovníka. Jeho pozícia by mala byť vyťažená od príchodu úlohou zavádzania čiarových kódov, predpoklad jeho ďalšieho využitia je zavedenie internetového obchodu.

Zvýšenie efektívnosti prinesie aj nákup čítačiek čiarových kódov; zmizne potreba fyzického prenosu informácií, naopak vznikne zjednodušenie práce, jednoduchšie

spätné dohľadanie chýb v evidenciách a zrýchlenie obsluhy zákazníka. Očakáva sa aj zníženie nákladov z dôvodu poklesu reklamácií a lepšie výstupy pre inventúru. Používaním Office 365 by mali byť zabezpečené všetky dáta pracovníkov vytvorené v tomto balíku.

Vplyvom navrhnutých opatrení sa podarilo znížiť všetky riziká, ktoré ohrozovali bezpečnostný a plynulý chod informačného systému organizácie. Ako sprievodný efekt sa znížili aj ostatné riziká. Nasledujúci graf zobrazuje počiatočnú významnosť rizík, ktoré sa podarilo znížiť z vysokej miery na prijateľnú a nové hodnoty rizík nemajúce kritický vplyv na IS.



Graf 1 Významnosť rizík pred a po návrhoch riešení
(Zdroj: Vlastné spracovanie)

ZÁVER

Správne fungovanie a konkurencieschopnosť spoločnosti je v dnešnej dobe signifikantne podmieňované využívaním informačných technológií. Správne zvolený a vybalansovaný informačný systém podporuje podnikové procesy a zefektívňuje prácu v podniku. Pokiaľ spoločnosť vníma informačné technológie ako nutné zlo, je pravdepodobné, že neuspeje v konkurenčnom boji.

Hlavným cieľom diplomovej práce bolo analyzovať zavedený informačný systém spoločnosti MARS, po celkovej analýze nájsť hrozby systému a z nich plynúce riziká a navrhnúť vhodné zmeny k eliminácií a zlepšeniu identifikovaných rizík. V teoretickej časti sú na základe štúdia odbornej literatúry vymedzené všetky dôležité pojmy týkajúce sa problematiky informačných systémov a technológií, a slúžia ako podklad pre analytickú a návrhovú časť.

Analýza informačného systému spoločnosti bola vykonaná pomocou vlastného skúmania, rozhovormi s majiteľom a pracovníkmi spoločnosti. Boli využité dve metódy hodnotenia informačného systému, pre ktoré bol využitý portál Zefis. Použila sa metóda HOS 8 a hodnotenie efektívnosti informačného systému. Boli zistené výrazné nedostatky najmä v oblasti bezpečnosti a spôsobu využívania systému, ale aj v ostatných oblastiach. Niektoré z týchto nedostatkov ohrozovali svojou podstatou bezpečný chod informačného systému a vyžadovali si okamžité riešenia. Výpis všetkých rizikových faktorov bol východiskom pre návrhy riešení, súčasťou ktorého bolo zostavenie analýzy rizík v zhode s metódou ISO/IEC 27005:2008 a kvantitatívne posúdenie najvýznamnejších hrozieb pre firmu. K eliminácií týchto rizík boli navrhnuté viaceré opatrenia, ktorých vplyv sa odzrkadlil aj na menej významných rizikách. Je možné konštatovať, že informačný systém je dnes v spoločnosti bez akejkoľvek koncepcie. Navrhované zmeny sa preto sústredili na návrhy opatrení koncepčných a systémových, ktoré by mali byť pevným základom pre spoločnosť, pre jej ďalší rast a prípadnú implementáciu internetového obchodu. Momentálne je potrebné predovšetkým vypracovať informačnú stratégiu spoločnosti, určiť metriky hodnotení, zaistiť efektívne využívanie aktuálneho systému, zabezpečiť ho proti hrozbám a pripraviť na ďalší rast podniku.

ZOZNAM POUŽITEJ LITERATÚRY

BASL, Josef a Roman BLAŽÍČEK. *Podnikové informační systémy: podnik v informační společnosti*. 3., aktualiz. a dopl. vyd. Praha: Grada, 2012, 323 s. ISBN 978-80-247-4307-3.

BÉBR, Richard a Petr DOUCEK. *Informační systémy pro podporu manažerské práce*. Praha: Professional Publishing, 2005. ISBN 80-86419-79-7.

ČSN ISO 9001:2001. *Systémy managementu jakosti – Požadavky*. Praha: Český normalizační institut

ŠLAPÁK, Ondrej. *Data, informace, znalosti*. E-LOGOS [online]. 2003 [cit. 2016-05-01]. Dostupné z: http://nb.vse.cz/kfil/elogos/miscellany/slapa103.pdf

ČANDÍK, Marek. *Informační bezpečnost*. CYBERSECURITY [online]. 2010 [cit. 2016-05-01]. Dostupné z: http://www.cybersecurity.cz/data/candik2.pdf

DĚDINA, Jiří a Václav CEJTHAMR. *Management a organizační chování: manažerské chování a zvyšování efektivity, řízení jednotlivců a skupin, manažerské role a styly, moc a vliv v řízení organizací*. Praha: Grada, 2005. Expert (Grada). ISBN 80-247-1300-4.

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

KOCH, Miloš a Viktor ONDRÁK. *Informační systémy a technologie*. Vyd. 1. Brno: Akademické nakladatelství CERM, 2004, 166 s. ISBN 80-214-2725-6.

KOCH, Miloš a kol. *Management informačních systémů*. Vyd. 3., přeprac. Brno: Akademické nakladatelství CERM, 2010, 171 s. ISBN 978-80-214-4157-6.

KOCH, Miloš. *ZEFIS - Výzkumný portál Ústavu informatiky Fakulty podnikatelské VUT v Brně* [online]. 2016 [cit. 2016-05-01]. Dostupné z: www.zefis.cz.

MOLNÁR, Zdeněk. *Efektivnost informačních systémů*. 2. rozš. vyd. Praha: Grada, 2001, 179 s. ISBN 80-247-0087-5.

MOLNÁR, Zdeněk. *Manažerské informační systémy*. Vyd. 1. V Praze: České vysoké učení technické, 2010, 116 s. ISBN 978-80-01-04596-1.

RÁBOVÁ, Ivana. *Podnikové informační systémy a technologie jejich vývoje*. Brno: Tribun EU, 2008. ISBN 978-80-7399-599-7.

SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 4. vydání. Praha: Grada Publishing, 2013. 488 s. ISBN 978-80-247-4644-9.

SODOMKA, Petr. *Informační systémy v podnikové praxi*. 2. Aktualiz. a rozš. vyd. Brno: Computer Press, a.s., 2010. 501 s. ISBN 978-80-251-2878-7.

SKŘIVÁNEK, František. *Databázový svět* [online]. 2004 [cit. 2016-02-01]. Dostupné z http://www.dbsvet.cz/view.php?cisloclanku=2008051401

ŠMÍDA, Filip. *Zavádění a rozvoj procesního řízení ve firmě*. Praha: Grada, 2007. Management v informační společnosti. ISBN 978-80-247-1679-4.

TICHÝ, Milík. *Ovládání rizika: analýza a management.* V Praze: C.H. Beck, 2006. Beckova edice ekonomie. ISBN 80-7179-415-5.

TVRDÍKOVÁ, Milena. *Zavádění a inovace informačních systémů ve firmách*. 1. vyd. Praha: Grada, 2000, 110 s. ISBN 80-7169-703-6.

VEBER, Jaromír. *Management: základy, prosperita, globalizace*. Praha: Management Press, 2000. ISBN 80-7261-029-5.

Účtovný program money S3. Vlastnosti systemu [online]. 2016 [cit. 2016-05-01]. Dostupné z: http://www.money.sk/money-s3/vlastnosti-systemu/

Účtovný program money S3. Technické informace Money s3 [online]. 2016 [cit. 2016-05-01]. Dostupné z: http://www.money.cz/navod/technicke-informace-money-s3/#minimalni-konfigurace-pro-jeden-pocitac

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK

ZOZNAM GRAFOV

ZOZNAM SKRATIEK

HW Hardware

SW Software

IS Information System

IT Information Technologies

NC Numerical Controlled

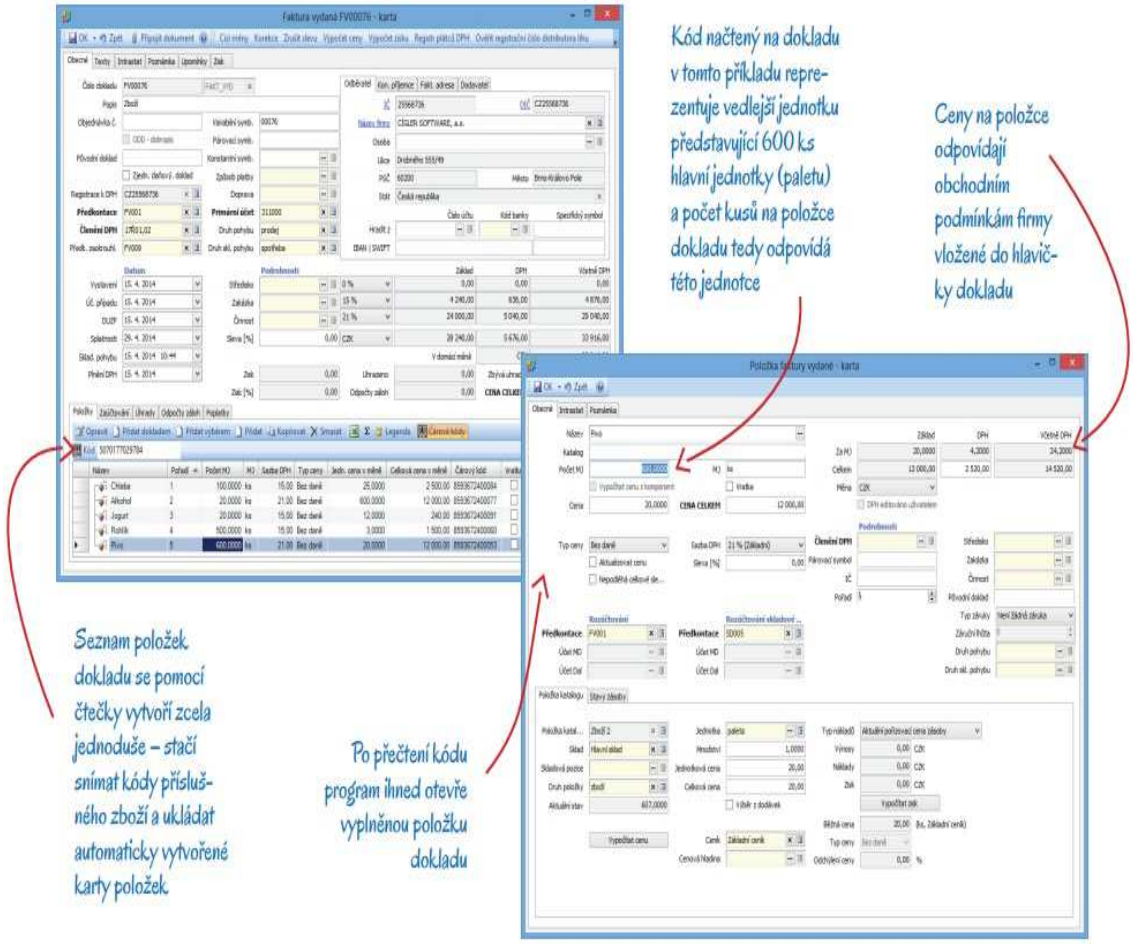
OS Operating System

ZOZNAM PRÍLOH

Príloha I: Vytváranie dokladov pridávaním položiek prostredníctvom skenerov

Príloha II: Ukážka vybraného skeneru

Príloha I: Vytváranie dokladov pridávaním položiek prostredníctvom skenerov



Príloha II: Ukážka vybraného skeneru

Názov produktu: PM8300-DK910RK10
Výrobca: Datalogic
CPU: IntelXScale PXA270 @312Mhz
Napájanie, doba chodu: Li-Ion 2150mAh; chod 10hodín/60 000 skenov
Pripojenie: WLAN 802.11a/b/g;
Display: Dotykový, 16 kláves
Dekódovacie shcopnosti: lineárne aj 2D kódy
Cena: ~800€
Ďalšie vlastnosti: odolnosť v náročných podmienkach ako mráz, vlhkosť, teplo, nárazy, prašnosť, pády