VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV MANAGEMENTU
INSTITUTE OF MANAGEMENT

POSOUZENÍ INFORMAČNÍHO SYSTÉMU FIRMY A NÁVRH ZMĚN
INFORMATION SYSTEM ASSESSMENT AND PROPOSAL OF ICT MODIFICATION

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Štěpán Novotný**
AUTHOR

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

BRNO 2022

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav managementu
Student:	**Bc. Štěpán Novotný**
Vedoucí práce:	**doc. Ing. Miloš Koch, CSc.**
Akademický rok:	2021/22
Studijní program:	Strategický rozvoj podniku

Garant studijního programu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

Posouzení informačního systému firmy a návrh změn

Charakteristika problematiky úkolu:

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

Cíle, kterých má být dosaženo:

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.

Základní literární prameny:

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.

GÁLA, Libor, Jan POUR a Zuzana ŠEDIVÁ. Podniková informatika. 2. přeprac. a aktualiz. vyd. Praha: Grada. 2009, 496 s. ISBN 978-80-247-2615-1.

MOLNÁR, Zdeněk. Efektivnost informačních systémů. 2. rozš. vyd. Praha: Ikar, 2000. 178 s. ISBN 80-247-0087-5.

SCHWALBE, Kathy. Řízení projektů v IT. Brno: Computer Press, 2007. 720 s. ISBN 978-80-251-1526-8.

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

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2021/22

V Brně dne 28.2.2022

L. S.

doc. Ing. Vít Chlebovský, Ph.D. garant	doc. Ing. Vojtěch Bartoš, Ph.D. děkan

Abstrakt

Diplomová práce se zabývá posouzením současného stavu informačního systému vybraného sociálního podniku působícího v oblasti poskytování outsourcingu administrativy. Na základě zjištění z provedených analýz a provedeného primárního empirického výzkumu je zhodnocen stav efektivnosti a zejména bezpečnosti podnikového informačního systému. Výsledkem této práce je vypracovaní plánu implementace nového systému a návrh změn a opatření vedoucích k eliminaci identifikovaných nedostatků a zmírnění potenciálních rizik.

Abstract

The diploma thesis deals with the assessment of the current state of the information system of a selected social enterprise operating in the field of administration outsourcing. Based on the findings of the analyses and primary empirical research, the state of efficiency and especially security of the enterprise information system is evaluated. The result of this work is the development of a plan for the implementation of the new system and the proposal of changes and measures leading to the elimination of identified deficiencies and mitigation of potential risks.

Klíčová slova

informační systém, informační bezpečnost, kybernetická bezpečnost, implementace, gamifikace, ZEFIS

Keywords

information system, information security, cyber security, implementation, gamification, ZEFIS

Bibliografická citace

NOVOTNÝ, Štěpán. *Posouzení informačního systému firmy a návrh změn* [online]. Brno, 2022 [cit. 2022-05-09]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/142523. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav managementu. Vedoucí práce Miloš Koch.

Čestné prohlášení

Prohlašuji, že předložená diplomová práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 9. května 2022

……

podpis autora

OBSAH

ÚVOD

Informační systémy (IS) jsou nedílnou součástí takřka většiny podniků ve všech odvětvích a procházejí vývojem společně s rozvojem informačních a komunikačních technologií (ICT). Projevují se prakticky ve všech aspektech lidského života a jejich využívání se dnes bere již jako naprostá nezbytnost a samozřejmost, s čímž se dostává do popředí i management IS. Informační technologie jsou dynamicky se rozvíjející obor, v němž dochází k neustálému zkracování inovačních cyklů. Nové technologie umožňují zásadním způsobem ovlivnit výkonnost podniků a otevírají tak zcela nové možnosti k dosažení strategických cílů. IS přispívají ke zefektivňování podnikových procesů, jelikož množství informací neustále narůstá. Cílem je dostat správné informace ve správný čas na správné místo, přičemž schopnost efektivně využívat podnikové informace je jedním z klíčových aspektů konkurenceschopnosti. Bez dostupnosti kvalitních informací lze jen stěží učinit kvalifikovaná rozhodnutí. Podniky si od jejich zavádění slibují zejména úsporu času a snížení nákladů, tyto ekonomické přínosy se však v praxi obtížně determinují a kvantifikují.

Posuzování podnikových informačních systémů je komplexní disciplínou vyžadující značné mezioborové znalosti. Problematika managementu IS totiž nespočívá pouze v implementaci stále pokročilejších a dokonalejších informačních systémů, ale především v jejich vhodném propojení se schopnostmi a znalostmi pracovníků. Informační systém je pouze tak efektivní, jako jeho nejslabší článek, což platí zejména pro jeho bezpečnost.

Otázka informační bezpečnosti je s přibývajícím výskytem nových hrozeb stále aktuálnější. Jejich spektrum je v oblasti IS/ICT enormně široké a rizika jsou pouze obtížně kvantifikovatelná. Rozsah a nároky na informační bezpečnost se značně liší dle významnosti podnikových dat. Ideální řešení je často o hledání kompromisu mezi zájmem organizace a přílišným omezováním uživatelů. Zavádění nejrůznějších opatření vyžaduje pokročilé znalosti, značné investice a kvalitní personální zajištění. I z těchto důvodů je problematika informační bezpečnosti často opomíjenou oblastí řízení a managementu IS v mnohých podnicích nevěnuje dostatečná pozornost.

1 CÍLE PRÁCE, METODY A POSTUPY ZPRACOVÁNÍ

Hlavním cílem této práce je posouzení, resp. analýza stávajícího stavu informačního systému, jeho efektivnosti a zejména bezpečnosti ve společnosti sales24, s.r.o., v prostředí specifického rychle se rozrůstajícího sociálního podniku, který působí v oblasti outsourcingu administrativy. Cílem je návrh změn, směřujících ke zlepšení stávajícího stavu a eliminaci nalezených rizik s důrazem na problematiku informační a kybernetické bezpečnosti.

Výzkum v této práci je zaměřen výlučně na pracovníky administrativního týmu a managementu, nezahrnuje tudíž zaměstnance pracující na zařízeních a v informačních systémech klientů, typicky bankovních institucí, jejichž funkcionalita a úroveň je značně odlišná.

V teoretické části, resp. literární rešerši budou vymezena základní východiska a elementární pojmy, jakožto i současné trendy, například gamifikace nebo cloud computing. V této části budou také vysvětleny principy analytických metod a použitých nástrojů. Po představení společnosti dojde k aplikaci analytických metod zaměřených na předmětný podnik a jeho okolí (SLEPTE, Porterův model pěti sil, Analýza 7S, Analýza stakeholderů ad.) a poté i na zkoumaný IS (tj. McFarlanův model, metoda ZEFIS ad.). V rámci analýzy bude také realizován primární empirický výzkum, který si klade za cíl zhodnotit stav informační bezpečnosti, identifikovat nedostatky a navrhnout zlepšení. V rámci tohoto výzkumu bude zvolen kvalitativní přístup pomocí techniky individuálních částečně strukturovaných rozhovorů. Výsledky analýz a primárního výzkumu budou následně sumarizovány prostřednictvím SWOT matice IS.

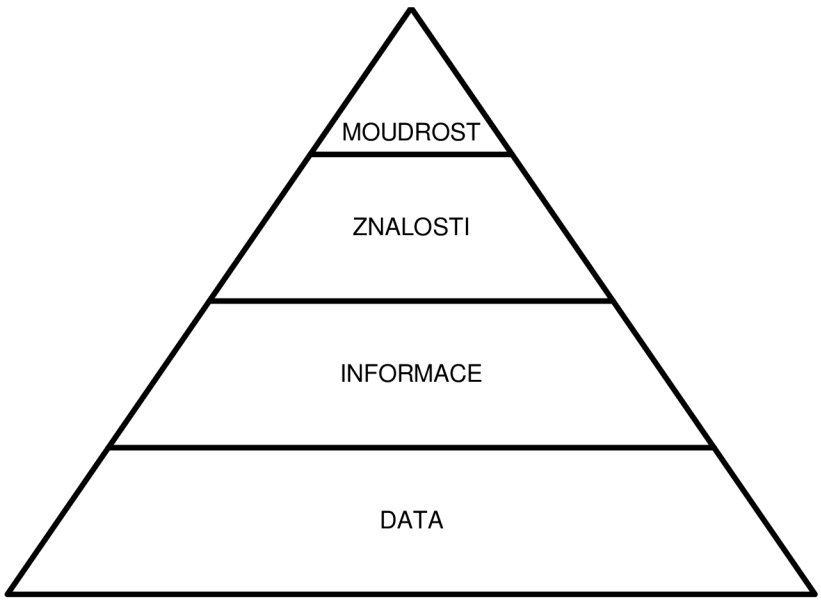
Na základě identifikovaných nedostatků budou sestaveny vlastní návrhy a tato změna bude popsána prostřednictvím Lewinova modelu, včetně časového plánu a analýzy rizik. Výstupem navrhovaných řešení budou i další změny, zejména organizačního a technického charakteru, a specifikace přínosů včetně stručného ekonomického zhodnocení. Realizace těchto návrhů a opatření povede ke zlepšení stavu bezpečnosti a efektivnosti podnikového informačního systému, což může v dlouhodobém horizontu vést ke zvýšení konkurenceschopnosti předmětného podniku.

2 TEORETICKÁ VÝCHODISKA PRÁCE

V teoretické části jsou vymezena základní východiska a elementární pojmy, jakožto i současné trendy, jakými je například gamifikace nebo cloud computing. V této části jsou také vysvětleny principy analytických metod a nástrojů použitých v praktické části této práce.

2.1 DIKW model

Model DIKW neboli DIKW pyramida, či informační hierarchie, je dle Rowleyové (2007) informační model vysvětlující strukturní a funkční vztahy mezi daty, informací, znalostí a moudrostí. Z tohoto modelu vyplývá, že primárním základem jsou data, za pomocí kterých můžeme zformulovat informace a na základě informací znalosti, které jsou výchozím předpokladem moudrosti. Společně s růstem míry lidského zapojení, tedy s postupem „vzhůru“ v pyramidě, klesá možnost algoritmizace.



Obrázek č. 1: DIKW pyramida
(Zdroj: vlastní zpracování dle Rowleyové, 2007)

2.1.1 Informace

Samotný výraz *informace* pochází z latinského *informatio*, resp. *informare* a je poprvé zaznamenán v roce 1274 (Gála, Pour a Šedivá, 2009). Molnár (2001) i Šilerová (2017) definují informaci jako „*data, kterým jejich uživatel přisuzuje určitý význam a které*

uspokojí konkrétní objektivní informační potřebu svého jedince“. Definic je v literatuře celá řada, jelikož jejich tvůrci kladou důraz na různé úrovně pohledu – např. syntaktický pohled je orientován na vnitřní strukturu informace bez ohledu na vztah k příjemci, sémantický pohled zdůrazňuje její význam, ovšem rovněž bez vztahu k příjemci, avšak pragmatický pohled již směřuje k praktickému využití informace, a tedy i jejímu významu pro příjemce (Sodomka a Klčová, 2010). V souvislosti s požadavky na dostupnost informací se hovoří o tzv. kritických informačních potřebách, které jsou nezbytné pro zajištění činnosti subjektu (Šilerová, 2017). Informace je určitá zpráva o nastalém jevu, který u příjemců snižuje míru neznalosti (Gála, Pour a Šedivá, 2009). Hodnota informace je pro příjemce subjektivní.

Informací je tedy každý nový poznatek, který má charakter výroku, lze tedy říci, zda je pravdivý či nikoli. Tyto poznatky disponují specifickými vlastnostmi – např. v procesu použití u nich nedochází ke spotřebě. Nositeli informace může být text, obraz, zvuk či číselná data (Šilerová, 2017). Autorka dále informace dělí do vzájemně protikladných dvojic na: potenciální (máme k dispozici, ale nepoužíváme) a aktuální, užitečné a škodlivé (tj. znemožňující dosažení cíle) a v poslední řadě také horizontální (poskytované na jedné úrovni řízení) a vertikální. Dobrá, kvalitní informace by měla naplňovat následující atributy (Šilerová, 2017):

1. relevance (charakter by měl odpovídat charakteru užití),
2. správnost (pravdivost, spolehlivost, přesnost),
3. včasnost (poskytování v době jejich potřeby),
4. aktuálnost (reflektování aktuální skutečnosti),
5. úplnost (veškeré požadované informace),
6. přiměřenost (přiměřená podrobnost),
7. nákladová přiměřenost (přiměřená doba a vynaložené náklady).

Kvalitu informace lze tedy posuzovat s pomocí řady ukazatelů jako je např. její zastaralost, chybnost (při zpracování či komunikaci), nespolehlivost, využitelnost či dostupnost. Kvalitě informací přispívá, nedochází-li k informačnímu přetížení (tj. přehlcení informacemi). (Šilerová, 2017) Jednou z překážek pro užívání informace je fakt, že většina informací je používána v jiné době a na jiném místě, než je místo jejího

vzniku, a navíc informace relevantní k jednomu účelu většinou navíc vznikají na vícero místech, ale především v různé struktuře (Šmída, 2007).

Zdroje informací pak mohou být z pohledu jejich místa vzniku interní nebo externí (tj. z okolí podniku). Soubor odborně zpracovaných informací v určitém systému lze označit jako informační fond. Informace získané z různorodých zdrojů se používají pro různé úrovně řízení – úroveň informací, resp. parametry získaných dat, jsou odlišné pro každou řídící úroveň. Kupříkladu informace pro operativní úroveň mají povětšinou tyto vlastnosti: nízký stupeň agregace, značná přesnost, aktuálnost, vysoká periodicita atp. Naopak informace pro strategickou úroveň řízení vykazují většinou vysoký stupeň agregace, perspektivnost, méně častou periodicitu apod. Operativní úroveň tedy klade značně vyšší nároky na technické zabezpečení procesu. (Šilerová, 2017) Základem každé informace jsou určité znaky. Přenos informace, tj. její výměna, je předmětem komunikace (Gála, Pour a Šedivá, 2015). Komunikace je kritickou fází v procesu, ve kterém si informace začnou stávat užitečnými a využitelnými. Významnou roli v tomto procesu hrají informační zdroje, které v dnešní době rychlého technologického růstu mění svoji povahu i modely svého fungování. Pro efektivní práci s informacemi je nezbytná informační gramotnost, což je schopnost porozumět informacím a využívat informace zobrazené v rozličných prostředích a formátech. Pojem informační gramotnosti v současnosti úzce souvisí i s počítačovou gramotností, jejíž osvojení je nutnou podmínkou. Oblast informační gramotnosti je však mnohem širší, jelikož vyžaduje schopnost příjemce získané informace zpracovat a využít pro zkvalitnění rozhodování. (Šilerová, 2017) Důležitost informační gramotnosti nabývá v současnosti na významu, jelikož kvantita dostupných informací významně předčí jejich kvalitu.

2.1.2 Data

Data jsou formalizované záznamy lidského poznání pomocí symbolů – znaků (Rosický, 2010), které jsou schopny přenosu, uchovávání, interpretace a zpracování (Gála, Pour a Šedivá, 2015). Hlavní rozdíl mezi informacemi a daty je tedy ten, že na rozdíl od dat nemůžeme informaci skladovat. Informace tedy vznikají z dat až v okamžiku jejich užití, kdy snižují entropii systému (Molnár, 2001). Data samotná však nebudou mít pro své příjemce hodnotu, postrádají-li schopnost z nich extrahovat informace. Data jsou tedy uživateli informací účelově shromažďována a myšlenkovými

procesy transformována tak, aby uspokojovali svoji informační potřebu spojenou s řešením konkrétního problému nebo přípravou rozhodnutí. (Šilerová, 2017) K problematice dat se váže i relativně nový pojem *Big data*, který bude diskutován v dalších kapitolách.

2.1.3 Znalosti

Informace v souvislostech (tj. kontextu) tvoří znalost, která reprezentuje porozumění získané zkušeností (či studiem) a je srozumitelná a použitelná k řešení problémů či rozhodování (Gála, Pour a Šedivá, 2015). Znalost je tedy tvořena množinou, resp. vzájemně provázanou strukturou poznatků a schopností reprezentovat data a informace. Znalosti jsou výsledkem aktivního procesu učení se. Systémy využívající znalosti se označují jako expertní systémy. *„Technologie pracují s daty, lidé je interpretují jako informace nesoucí význam, které se stávají předmětem pro další jednání. Proces interpretace je kognitivní záležitost, ve které stěžejní roli hrají znalosti.“* (Šilerová, 2017)

Dle využití můžeme znalosti dle autorky kategorizovat do tří elementárních skupin:

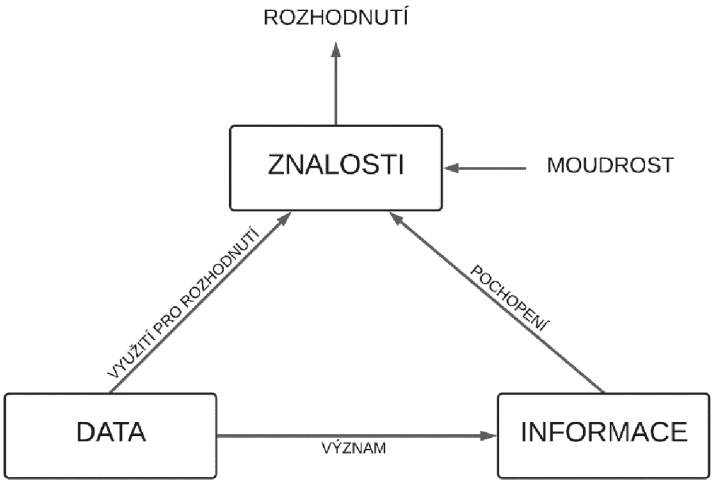
- tacitní znalosti – získané zkušeností, nevyslovené, nepoužité,
- explicitní znalosti – sdělitelné, formalizovatelné, uložené např. v IS),
- implicitní znalosti – individuální, získané zkušenostmi, praxí či studiem.

Někdy se v rámci znalostí hovoří i o zkušenostech. Dle Basla a Blažíčka (2012) mohou být zkušenosti informace, které nejsou dosud zaznamenány v nějaké databázi či jiné formalizované podobě – může se jednat například o zkušenosti zaměstnanců, které jsou využívané operativně v okamžiku potřeby. Takovéto informace jsou předmětem managementu znalostí.

2.1.4 Moudrost

Se zkušenostmi úzce souvisí i moudrost, která nám umožňuje říci, proč danou akci provedeme (Šilerová, 2017). Moudrost je z výše uvedených pojmů zřejmě nejhůře definovatelná. Rowleyová a Hartley (2008) popisují moudrost jako schopnost zvyšovat efektivitu, jelikož *„moudrost přidává hodnotu, která vyžaduje mentální schopnost posuzování“*. Moudrost vstupuje do procesu zpracování dat společně se znalostí a dle

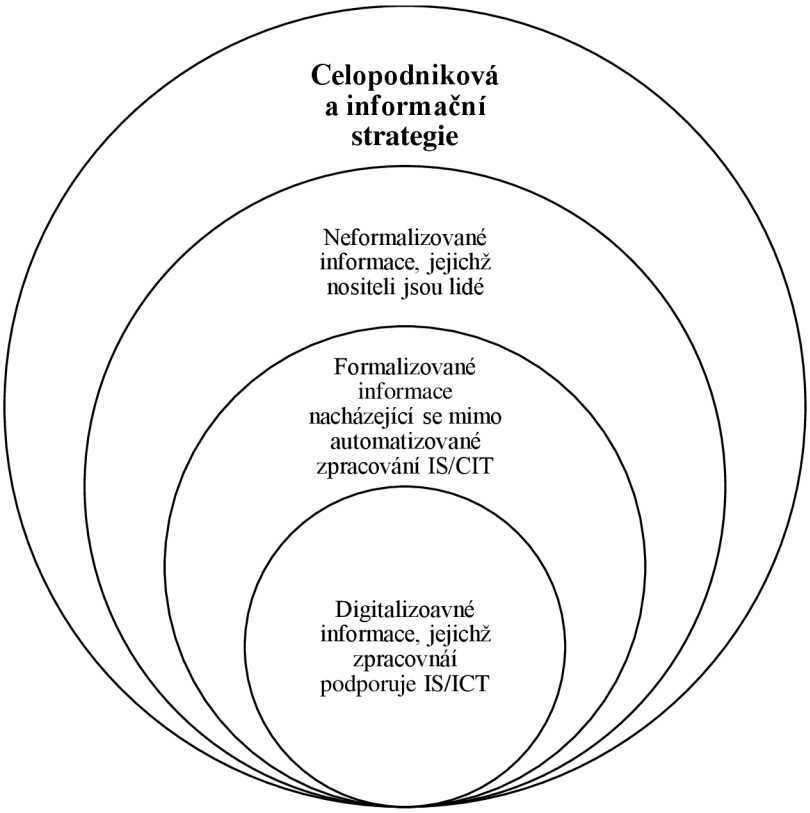
Šilerové (2017) představuje důvod, proč realizujeme mnohdy zcela odlišná rozhodnutí při dostupnosti stejných dat a informací.



Obrázek č. 2: Proces využití dat a informací
(Zdroj: vlastní zpracování dle Šilerové, 2017)

2.2 Informační strategie

Informační strategie (někteří autoři, např. Veber a Srpová (2012) operují s rozšířeným pojmem informační a komunikační strategie) má za účel formulovat základní koncept rozvoje podnikové informatiky, což znamená vymezit hlavní možnosti a úlohy jak po stránce technologické, tak organizační (Gála, Pour a Šedivá, 2009). Obecně informační strategií rozumíme soustavu cílů (např. zvyšování výkonnosti a zisk konkurenční výhody) a způsobů jejich dosažení (Molnár, 2001). Šilerová (2017) ji popisuje jako proces pomáhající zajistit optimalizaci procesu řízení budování, implementace a provozu informačního systému. Je tedy třeba definovat požadavky na IS tak, aby maximálně podporoval firemní procesy a byl v souladu se strategií podniku. Tyto požadavky se vyvíjejí jak podle potřeb organizace, tak i jednotlivých skupin. Je tedy nanejvýš nutné o nich přemýšlet s výhledem do budoucna. Nezanedbatelný vliv na ně mají také dynamicky se vyvíjející možnosti IT/ICT produktů, jejich přínosy jsou však často obtížně rozpoznatelné a manažeři je ne vždy dokáží identifikovat (Sodomka a Klčová, 2010). Informační strategie musí bezpodmínečně vycházet ze základních podnikových dokumentů, jakými je podniková strategie, organizační řád, interní pravidla apod. a kalkulovat s jejich vývojem. (Gála, Pour a Šedivá, 2009)



Obrázek č. 3: Formalizace informací a jejich automatizované zpracování
(Zdroj: vlastní zpracování dle Sodomky a Klčové, 2010)

„*Strategické řízení IS/ICT lze definovat jako kontinuální proces, jehož cílem je efektivně využít informačních systémů a technologií k vytváření přidané hodnoty produktů a služeb, které organizace nabízí zákazníkům*“ (Sodomka a Klčová, 2010). Informační strategie je základní nástroj, základní koncept, dlouhodobého řízení provozu a rozvoje PIS, je tedy součástí celého strategického řízení, vyžaduje tedy trvalý dialog mezi managementem a informatiky a skládá se obvykle z následujících částí (Gála, Pour a Šedivá, 2009):

- formulace základních cílů rozvoje informatiky (na základě cílů a požadavků),
- analýza současného stavu informatiky (SW, HW, trendy),
- návrh nového IS (zejm. na úrovni nových aplikací či tech. infrastruktury),
- definování způsobu realizace informační strategie (projekty, harmonogram realizace).

Šilerová (2017) uvádí, že vypracování informační strategie předpokládá absolvování několika postupných kroků:

1. ujasnění podnikatelské strategie – vyhodnocení všech záměrů,

2. zmapování a popsání procesů – vč. případných návrhů optimalizace,
3. vypracování informačních modelů podniku – modelů všech informací ve firmě,
4. definování funkčních požadavků – pracovníků, uživ. rozhraní, podpory procesů,
5. definování požadovaných přínosů – měřitelné i obtížně měřitelné,
6. stanovení požadavků na technologii – z několika hledisek,
7. specifikace projektů IT – určení zásadních projektů pro realizaci,
8. stanovení priorit – dle přínosů pro podnik a finančních možností.

Sodomka a Klčová (2010) výše uvedené body shrnují do tří klíčových kroků – analyzovat a zhodnotit současný stav IS/ICT, definovat cílový stav IS/ICT a navrhnout postup, jak tohoto cílového stavu dosáhnout za klíčových podmínek. Obvyklý je výběr několika variant řešení IS, přičemž svoji roli hraje velké množství kritérií, jako je nejen cena, ale také funkčnost či bezpečnost (Veber a Srpová, 2012).

Neexistence informační strategie podniku je jednou z hlavních příčin vynakládání neefektivních výdajů na IS/IT, což se projevuje např. zbytečným či neúčelným nákupům hardware i software, které se posléze ukázaly jako rychle zastarávající, nepotřebné či vzájemně nekompatibilní. Jedním z hlavních faktorů neúspěchu při implementaci informačních systémů bývá nedokonalé strategické řízení IS/ICT, které často stále zůstává na okraji zájmu manažerů, což je ovlivněno mj. nevyhovujícím zařazením informatiky v organizační struktuře podniku (Šilerová, 2017). V rámci procesu tvorby informační strategie je nezbytné, aby byly pro každý projekt jasně definované cíle, přičemž by měly být SMART, tedy přesně stanovené, měřitelné, výstižné, realistické a časově ohraničené (Sodomka a Klčová, 2010). Je také třeba, aby bylo uvažováno s celým generickým portfoliem, byly definovány metriky, resp. portfolio metrik, určený zodpovědný manažer, stanoven časový a organizační harmonogram a zejm., aby bylo veškeré toto očekávání vč. veškerých opatření komunikováno s dotčenými pracovníky. Do prvotní fáze tvorby informační strategie spadá zejména hloubková analýza podmínek, definice kritických faktorů rozvoje, formulace informačních potřeb a návrh pravidel pro rozvoj IS/IT. Kvalitní informační strategie stojí na dvou aspektech – na porozumění mezi manažery a informatiky a na dohodě všech klíčových pracovníků (Šilerová, 2017). Při stanovování informační strategie podniku by se měl klást důraz na zvýšení informační gramotnosti manažerů,

a zvláště pak na zajištění jejich osobní angažovanosti v problematice rozvoje informačních systémů a technologií v podniku. (Molnár, 2001)

Obsah podnikové informační strategie je do značné míry závislý zejména na implementaci Corporate Governance, který definuje pravidla a rámec řízení (Koch, 2010). Korektně vypracovaná, vedením schválená a celým podnikem adaptovaná informační strategie se v počáteční fázi životního cyklu informačních systémů používá zejména jako základ pro zadávání dílčích projektů (např. pořízení HW či dílčích modulů IS), jejich koordinaci a kontrolu, avšak také urychluje řešení implementace (Šilerová, 2017). Využívá se také pro zpracování poptávky u výběrových řízení na dodavatele IS/IT a obsahuje koncepční podklady pro plánování investic do IS/ICT (Sodomka a Klčová, 2010). Podniková informační strategie se používá i v dalších životních fázích IS a to především pro kontrolu plnění strategie a kontinuální pravidelné aktualizace.

2.3 Informační systém

Systém lze obecně chápat jako soubor podstatných znalostí o vytyčené části reálného světa zapsaných ve vhodném jazyce, přičemž je tvořen prvky a závislostmi mezi nimi, tj. vazbami. (Gála, Pour a Šedivá, 2015). Molnár (2001) definuje systém jako uspořádanou množinu prvků spolu s jejich vlastnostmi a vztahy, které vykazují určité vlastnosti (chování) celku. U takto definovaného systému (s cílovým chováním) lze identifikovat především jeho: účel (tj. cílové chování), strukturu (prvky a vazby mezi nimi), vlastnosti prvků, vlastnosti vazeb, okolí systému (ovlivňující jeho chování) a případné subsystémy (je-li ho možné rozdělit). Účelem informačního systému je pak zajištění vhodného přenosu, zpracování a vyjádření informací. (Gála, Pour a Šedivá, 2009) Basl a Blažíček (2012) informační systém definují jako „*soubor lidí, technických prostředků a metod zabezpečujících sběr, přenos, uchování a zpracování dat za účelem tvorby a prezentace informací pro potřeby uživatelů činných v systémech řízení.*“ Informační systém je tedy nejen množinou formalizovaných informací v podniku, ale jsou to též prostředky a postupy umožňující tyto informace vyhledávat, ukládat a distribuovat. Informatika, potažmo informační systémy, našly své uplatnění prakticky ve všech oblastích lidské činnosti, což má přímý vliv na komplexnost takovýchto systémů (Šilerová, 2017). Úlohou informačních systémů v podnicích je zejména

podpora interních podnikových procesů, přičemž by měl být brán zřetel na stanovenou informační strategii. Efektivně fungující podnikový informační systém je jedním ze strategických faktorů ovlivňující konkurenceschopnost firmy.

Co bývá v praxi často opomíjeno, je definování rámce podnikových informačních systémů, resp. postavení informačních a komunikačních technologií (ICT) v tomto rámci. Informace se totiž mohou, jak již bylo zmíněno výše, vyskytovat v několika různých podobách, na různých nosičích. Z tohoto důvodu, ze třech různých druhů nosičů, lze odvodit tři roviny chápání informačního systému (Basl a Blažíček, 2012):

Obrázek č. 4: Roviny chápání informačního systému v podniku
(Zdroj: vlastní zpracování dle Basla a Blažíčka, 2012)

Jedná se o tzv. holistický pohled na informační systém, který je mnohem širší a komplexnější, jelikož nezahrnuje pouze automatizovanou část systému (Koch, 2010). „*Informační systémy se v podniku nevyskytují totiž jen v souvislosti s ICT, ale v širším rámci mohou být vnímány s ohledem na míru formalizace údajů, podíl lidského faktoru i například s ohledem na druh „nosičů" informací.*" (Basl a Blažíček, 2012)

2.3.1 Podnikový informační systém

Podnikový informační systém (PIS) je otevřený systém, jehož vstupy a výstupy jsou informace, přičemž kromě své formální podoby (pravidla, předpisy) má i podobu

neformální, reprezentovanou výměnou a zpracováním informací lidmi (komunikace) (Gála, Pour a Šedivá, 2015). Úlohou PIS je podpořit zejména primární cíle podniku, ovlivnit jeho konkurenceschopnost a postavení podniku na trhu (Šilerová, 2017). V českém prostředí se můžeme povětšinou setkat se dvěma základními přístupy formující očekávání od podnikového informačního systému – ten většinový chápe PIS především jako podpůrný nástroj pro řízení, druhý přístup se pak opírá i o požadavky směřující do oblastí, které nesouvisí pouze s IS, ale zohledňují také změny v organizační struktuře a řízení, standardizaci procesů či sdílení best practises (Sodomka a Klčová, 2010).

Informační systém, resp. PIS, představuje konzistentně uspořádanou množinu komponent spolupracujících za účelem tvorby, shromažďování, zpracování, přenášení a rozšiřování informací. Prvky informačního systému jsou lidé (uživatelé) a informatické zdroje. (Hindls, Hronová a Holman, 2003). Nicméně například Gála, Pour a Šedivá (2015) tento výčet rozšiřují explicitně o informační technologie (IT), data, řízení a transformační proces. Sodomka a Klčová (2010) shrnují poslání podnikového informačního systému do třech hlavních bodů:

- integrující platforma spojující podnikové procesy,
- nositel standardizace,
- poskytování celostního pohledu na fungování organizace.

Rozdílné požadavky jednotlivých úrovní řízení, popř. podnikových úseků na nasazení různých aplikací lze do jisté míry vyřešit jejich integrací, která umožní provázané řízení podnikových procesů a zpracování informací v podniku jako celku. Správně fungující podnik se neobjede bez zavedení systému a řádu do rutinních činností probíhajících v organizaci. Roli sjednocujícího prvku, jakéhosi nositele standardizace, by v tomto případě měl sehrát právě správně nastavený informační systém, který bude mj. sloužit k formalizaci informací a jejich zpracování za účelem poskytování relevantních výstupů. (Sodomka a Klčová, 2010) Mezi důležité rysy podnikových informačních systémů patří dle Šilerové (2017):

- management znalostí – znalostní kapitál jakožto zdroj podniku – informační logistika jejíž základem jsou datové sklady (Data Warehouse), nástroje BI a podnikové portály,

- ochrana informací – informační bezpečnost finančních informací, dat zákazníků apod.,
- informační odpad – nepotřebné informace se kumulují, hrozí přehlcení informacemi, je nutné nastavit proces toku informací v podniku včetně nakládání s nepotřebnými záznamy.

„Podnikový informační systém vytvářejí lidé, kteří prostřednictvím dostupných technologických prostředků a stanovené metodiky zpracovávají podniková data a vytvářejí z nich informační a znalostní bázi organizace sloužící k řízení podnikových procesů, manažerskému rozhodování a správě podnikové agendy" (Sodomka a Klčová, 2010). *„Informační a komunikační systém lze charakterizovat jako soubor lidí, metod a technických prostředků zajišťujících sběr, přenos, uchovávání, zpracování a prezentaci zpráv a dat s cílem tvorby a poskytování informací dle potřeb jejich příjemců činných v systémech řízení"* (Veber a Srpová, 2012). Lidé, resp. uživatelé informačního systému, tedy představují významný prvek podnikového informačního systému a jsou základním kritickým faktorem úspěchu IT projektu (Sodomka a Klčová, 2010). Je třeba mít na paměti, že tím, co ovlivňuje postavení podniku v konkurenčním prostředí ve vztahu k IS je zejména schopnost pracovníků pracovat s daty, informacemi a znalostmi v systému obsaženém (Svozilová, 2011). Nelze se tedy soustředit pouze na softwarové a hardwarové vybavení, ale je třeba se soustředit na zlepšení všech procesů a činností v podniku. Sodomka a Klčová (2010) navíc upozorňují, že každý člověk je kromě svého vzdělání ovlivněn i zkušenostmi a čerpáním odborných informací z různě kvalitních zdrojů. Lidé jsou omylní, vnášejí do relativně racionální projektové činnosti emoce nebo špatně chápou prezentované informace. Panuje zde také chaos v dostupných informacích (vzhledem k faktu, že podniková informatika je relativně nový obor) a z toho plynoucí disproporce ve znalostech u jednotlivých pracovníků.

Uživatele podnikových informačních systémů můžeme rozdělit dle několika hledisek. Sodomka a Klčová (2010) je dělí do dvou kategorií na klíčové uživatele, zastřešující správu procesů a koncové uživatele, což jsou všichni pracovníci využívající podnikový IS. Šilerová (2017) uživatele IS kategorizuje obdobně, a to na koncové uživatele využívající informace (a podílející se na formulaci účelu) a IT personál, který provoz či údržbu IS, resp. PIS, zajišťuje. Řízení IS/IT, potažmo informatiky vyžaduje jak pečlivou pozornost vrcholového vedení, které je za kvalitu informačního systému zodpovědné,

tak spolupráci mezi jednotlivými podnikovými útvary. Realizuje se na 3 základních úrovních obdobně jako v jiných oblastech řízení podniku (Šilerová, 2017):

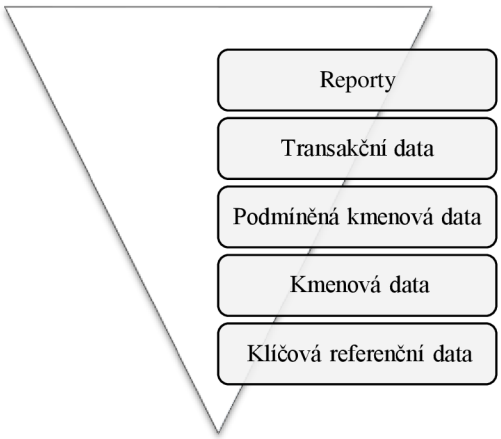
1. strategická úroveň řízení – formulace informační strategie, tvorba koncepce,
2. taktická úroveň řízení – řízení projektů, tvorba provozních předpokladů,
3. operativní úroveň řízení – řízení provozu, instalace a údržba.

Vývoj PIS je možno sledovat z několika pohledů – rozlišujeme tři základní modely PIS – z hlediska úrovní řízení, z hlediska technologického a z hlediska procesního. IS podle úrovní řízení je hodnocen dle toho, jak odpovídá potřebám řízení a obvykle se týkají všech třech úrovní. Jedná se o IS pro transakční zpracování, IS pro podporu rozhodování a strategické IS. Další možnou kategorizací je dělení dle technologického postupu (IS vyvíjen dle požadavků uživatelů) či z hlediska podnikových procesů. (Šilerová, 2017)

Podnikový informační systém je z datového pohledu možné dekomponovat do několika základních vrstev: hardware, operační systém, databázový systém a aplikační software. Tento přístup k pojetí IS se někdy označuje jako technologický, jelikož se znázorňuje pomocí na sebe navazujících vrstev. (Basl a Blažíček, 2012) Data obsažená v podnikovém informačním systému jde v zásadě rozdělit do třech klíčových skupin (Gála, Pour a Šedivá, 2015):

- data o společenských podmínkách podnikání (vnější faktory),
- data o trhu (poptávka, stav konkurence, …),
- interní data podniku (plány a predikce, vnitřní zdroje, pravidla).

Data podnikového informačního systému (PIS) se mohou dělit také dle své strukturovanosti (strukturovaná a nestrukturovaná), popř. se mohou rozlišovat reporty (data o stavu či hlášení), transakční data (vzniklá při realizaci transakcí), podmíněná kmenová data (podmínky a pravidla), kmenová data (údaje spojené s transformačním procesem podniku) a klíčová referenční data (údaje o zdrojích a schopnostech podniku). (Gála, Pour a Šedivá, 2015) Šilerová (2017) data dělí, z pohledu *Master Data Managementu*, na transakční, operativní a analytická.



Obrázek č. 5: Hierarchie podnikových dat
(Zdroj: vlastní zpracování dle Gály, Poura a Šedivé, 2011)

Basl a Blažíček (2012) dále specifikují pět základních skupin dat podnikového ERP – číselníky, kmenová data, zakázková data, archivní data a parametry. Z hlediska implementace a vlastního užívání PIS je možné dále členit data, resp. databáze na: provozní, školící a testovací.

2.3.2 Funkce IS

Data jsou buď zaznamenávána uživateli prostřednictvím aplikací nebo jsou získávána jinými způsoby (např. přenesena z jiné aplikace, popř. dodána jiným systémem – např. senzorem). Aplikace zajišťují, vyjma zachycení a uložení dat, i jejich zpracování a prezentaci. Tyto vlastnosti či části aplikace se označují jako logiky aplikace. Pro zajištění funkcionalit rozlišujeme tři základní logiky aplikace (Gála, Pour a Šedivá, 2015):

- prezentační logika – spojována s uživatelským rozhraním (záznam a prezentace dat),
- datová logika – dodávání dat, úložiště dat, příprava dat,
- aplikační logika – zpracování dat dle příslušného algoritmu.

Tyto tři logiky zároveň tvoří jádro tzv. třívrstvé architektury, kde je datová vrstva oddělená od vrstvy aplikační a prezentační (Basl a Blažíček, 2012). Existují v zásadě dva základní přístupy k ukládání dat – souborový přístup a databázový přístup. U souborového přístupu jsou údaje (data) o objektech jedné třídy umístěny do samostatného souboru, zatímco databázový přístup řeší některé nedokonalosti

souborového přístupu a umožňuje tak zachytit vzájemné vztahy mezi objekty či kombinovat různě strukturovaná data. Databázové systémy proto dnes představují dominantní přístup k ukládání dat v podnikových informačních systémech, přičemž nejužívanějších jsou relační databázové systémy (např. SQL) (Gála, Pour a Šedivá, 2015)

2.3.3 Architektura IS

Architektura informačních systémů vychází především z podnikové strategie, resp. z podnikových strategických cílů a potřeb vč. strategie informační. Architektura musí splňovat určité principy – musí být perspektivní a vzhledem k úzké spolupráci odborníků a koncových uživatelů pochopitelná a srozumitelná pro všechny, přičemž se počítá s její postupnou aktualizací a doplňováním. Důraz na architekturu informačních systémů je určen především rostoucí komplexností IS. Samotná architektura by měla podporovat určité vlastnosti, jakými je například integrovanost (funkční, datová, SW, HW, uživatelského rozhraní), otevřenost (SW, HW), uživatelská přijatelnost apod. Architekturu IS lze základně dělit na globální architekturu (tj. hrubý návrh IS vč. ICT) a dílčí architekturu (rozpracované, detailnější vzájemně propojené návrhy). (Šilerová, 2017) Globální architektura je základním schématem IS. Je tvořena jednotlivými bloky, které představují aplikace včetně jejich datových základen a ICT vybavení (Koch, 2010). Autor dále dělí architekturu informačních systémů na:

- funkční – rozděluje IS na subsystémy dle funkcionalit postupnou dekompozicí,
- procesní – zaměřuje se na popis budoucího stavu procesů (s důrazem na ext. události),
- technickou (HW) – definuje typy a rozmístění prostředků ICT,
- technologickou – určuje způsob zpracování jednotlivých aplikací v návaznostech,
- datovou – návrh datové základny organizace,
- programovou (SW) – určuje programy a programové komponenty,
- komunikační – definuje vnější rozhraní systému,
- řídící – určuje pravidla fungování systému (patří sem orgware).

Tvorbu vlastní architektury dle Šilerové (2017) dělíme do tří vrstev: prostředí (situace, podmínky, legislativa), aplikační (projektová dokumentace a pravidla) a technologická

(návrh komponent, struktury, vazeb, sítí, SW). Vytvořená architektura umožňuje snazší tvorbu a implementaci systému, stejně jako je významným komunikačním prvkem v celém procesu. Existence architektury tedy usnadňuje návrhy jednotlivých modulů IS a potenciálně vede i k finančním úsporám.

Sodomka a Klčová (2010) upozorňují na poněkud specifickou dvojí pozici manažerských informačních systémů (MIS) v podnikové architektuře. První, běžněji se vyskytující varianta spočívá ve výskytu MIS jakožto samostatně funkční jednotky plněné agregovanými daty z jednotlivých, zpravidla transakčních, systémů. Tento typ využívá výhradně agregovaná data, což nedovoluje vytvořit nad daty nové úhly pohledu, s nimiž se při budování MIS nepočítalo. Druhou variantou je moderní MIS, jenž řeší některé problémy standardních manažerských IS včetně zmíněného využívání výhradně agregovaných dat. Takovýto moderní systém dokáže v přijatelné časově odezvě reagovat na dotazy nad velkým množstvím dat i na dotazy týkající se detailů jednotlivých záznamů.

Je důležité si uvědomit, že každý podnik je v jiné situaci, ovlivňují ho různé (vnitřní i vnější) faktory, a tudíž využívá různých typů softwarových aplikací pro různé úrovně řízení, a to k plnění rozličných specifických funkcí. Procesy v každém podniku jsou taktéž do určité míry unikátní a pro daný podnik či odvětví specifické. Infrastruktura informačního systému, zvláště pak ICT, by měla být vhodně optimalizovaná.

2.3.4 Infrastruktura IS

Struktura podnikového informačního systému je základnou pro aplikace informačních technologií a zároveň prostředím pro uložení a zpřístupnění dat. Molnár (2001) či Veber a Srpová (2012) rozlišují pět hlavních komponent infrastruktury:

- hardware,
- základní software,
- dataware (datové zdroje),
- peopleware (informační a počítačová gramotnost uživatelů),
- orgware (adekvátní organizační uspořádání – nařízení a pravidla).

Informační technologie (IT) představují „*postupy a metody vyjádření, zachycení, zpracování, ukládání, uchovávání a přenášení informací*“ (Gála, Pour a Šedivá, 2015).

V zásadě je členíme na software (SW) a hardware (HW), tj. zařízení využívaná SW. Transformační proces podnikového IS je pak aplikace informačních technologií do podniku. K monitoringu infrastruktury a podpoře uživatelů slouží Service Desk, jehož smyslem je zajistit podporu koncovým uživatelům informačního systému, resp. identifikovat problém, přidělit jej někomu k řešení a kontrolovat jeho vyřešení (Koch, 2010). Úroveň infrastruktury informačního systému je dána úrovní jednotlivých dílčích komponent, přičemž pro efektivní systém je žádoucí, aby všechny komponenty byly na vzájemně odpovídající vyrovnané úrovni (Molnár, 2001). Infrastruktura podnikového IS využívá infrastrukturu podniku (tj. energie, zázemí, pravidla a směrnice), infrastrukturu segmentu trhu (standardy v oboru) a veřejnou infrastrukturu (telekomunikace apod.) (Gála, Pour a Šedivá, 2015).

Informační systémy podléhají různému stupni integrace – integrované IS zajišťují spolupráci celé řady dílčích modulů nutných k efektivnímu zajištění informační podpory pro provoz podniku a z tohoto důvodu integrace podnikových aplikací (*Enterprise Application Integration*, EAI) patří ke stěžejním tématům při realizaci IT projektů. (Sodomka a Klčová, 2010) Pro zajištění maximální efektivity IS se zvyšují požadavky na provázanost a spolupráci jednotlivých systémů a aplikací v podniku. *„Neintegrovaná architektura s sebou přináší mnoho duplicit a nekonzistentností v podnikových datech. (...) Kromě vzniku nadbytečných nákladů má roztříštěná infrastruktura dopad i na celkovou efektivnost zpracování informací v organizaci.“* (Sodomka a Klčová, 2010)

Možným řešením toho, jak zajistit, aby napříč podnikem byla ta „správná“ data – spolehlivé informace vytvářející obraz „jedné nezpochybnitelné pravdy“, je použití jednoúčelového rozhraní na transfer kritických dat mezi podnikovými aplikacemi. U velkých podniků se však může jednat o desítky takovýchto míst vyžadující separátní rozhraní, jejichž údržba může podnik neúměrně finančně zatěžovat. Takováto situace, kde je třeba pracovat s roztříštěnou strukturou aplikací, značně komplikuje efektivní řízení podnikových procesů. Koncepce systémové integrace by měla být již součástí dlouhodobě budované a uplatňované informační strategie. (Sodomka a Klčová, 2010) Informační strategie v podniku nezbytně slouží jako podklad pro budování IS/ICT a snižuje rizika neúspěchu. *„Pojem budování IS/ICT vyjadřuje skutečnost, že v dnešní*

době nejde jen o vývoj nového software, ale také o implementaci již hotových řešení, integraci různých systémů, subsystémů, komponent či služeb“ (Basl, 2011).

Systémová integrace je spojená také se změnou podnikových procesů. Systémový integrátor je tak dle Šilerové (2017) zodpovědný za provázanost IT/ICT systémů s procesy v podniku. Nese se sebou také možná rizika ve formě vyšší závislosti na dodavateli (který je zároveň systémovým integrátorem) jednotlivých komponent, resp. na kvalitě jeho služeb, vyšší složitosti komplexního systému a s tím spjaté vyšší nároky na uživatele a zásadnější následky případných chyb a dopad havárií. Rozlišujeme několik stádií či složek systémové integrace – datovou integraci (tj. propojení datových základen různých aplikací), integraci aplikací (vzájemná kompatibilita či skrze API), integraci podnikových procesů a funkcí, integraci uživatelských rozhraní a integraci HW a technologickou. Naopak Sodomka a Klčová (2010) nerozlišují již integraci HW a technologickou, nýbrž integraci na úrovni obchodní logiky, což je způsob značně zasahující do struktury stávajících podnikových aplikací.

2.3.4.1 Software

Jako software (někdy též programové vybavení) se označuje sada instrukcí, které říkají počítači, co má vykonat. V přeneseném významu je to souhrn všech počítačových programů používaných v počítači provádějících nějakou činnost. (Johnson, 2021) Software lze dle Gály, Poura a Šedivé (2015) členit například na:

- aplikační software (ASW) - aplikace IT v podniku,
- základní software (ZSW) - umožňující provoz IT aplikací,
- software podporující rozvoj IS, vývoj ASW a zajišťující podporu řízení provozu informačních systémů.

Aplikační software zahrnuje celou řadu běžně používaných aplikací, zatímco pod pojem základní software si lze představit například operační systém (OS). Nákup software je povětšinou realizován nákupem licencí, které jsou buď jednorázové nebo doživotní. V současné době je na vzestupu model pořízení SW prostřednictvím pronájmu (např. kancelářské balíky Microsoft Office).

2.3.4.2 Hardware

Pojmem hardware se označuje široká škála různých zařízení (počítačů a periferií), komunikačních zařízení, zařízení spotřební elektroniky a dílů a součástek (Gála, Pour a Šedivá, 2015). V užším slova smyslu pak označuje veškeré fyzicky existující technické vybavení počítače, jakým je například základní deska, grafická karta, RAM, zdroj atd. Zaměstnanci, resp. uživatelé podnikového informačního systému přistupují ke službám pomocí různých hardwarových komponent. Veber a Srpová (2012) dělí hardwarové součásti IS do následujících skupin:

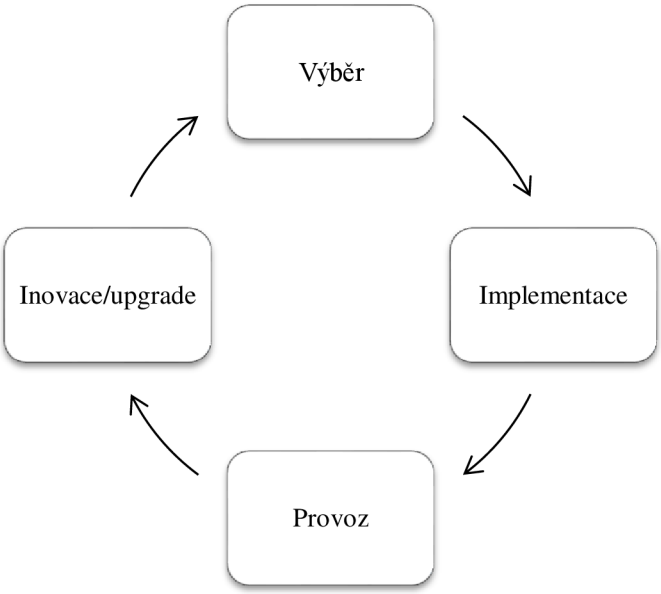
- koncové stanice,
- komunikační zařízení,
- periferní zařízení,
- prvky zajišťující datové propojení,
- servery.

2.3.5 Životní cyklus IS

Životní cyklus každého informačního systému prochází svými životními fázemi. Tento cyklus začíná již okamžikem, kdy se podnik rozhodne pro nový IS a trvá až do doby, kdy jej přestane využívat. Životní cyklus podnikového informačního systému lze obvykle rozdělit do čtyřech částí (Šilerová, 2017):

1. plánování,
2. návrh,
3. implementace,
4. provoz a údržba.

Typů životních cyklů IS lze definovat několik, procházejí však také vývojem společně s rozvojem informačních a komunikačních technologií. Například Basl a Blažíček (2012) namísto plánování a návrhu uvádějí pouze souhrnně „*výběr IS*“, který zahrnuje výběr vhodného řešení pokrývajícího podnikové potřeby a očekávání, po které následuje implementace a dále provoz. Posledním, čtvrtým bodem je inovace informačního systému, tj. buď upgrade systému nebo přechod na jiný produkt.



Obrázek č. 6: Životní cyklus IS v podniku
(Zdroj: vlastní zpracování dle Basla a Blažíčka, 2012)

Životní cyklus aplikace je dle Gály, Poura a Šedivé (2015) cyklický, což znamená, že se po určité době, po průchodu vývojovými fázemi, vrací zpět na svůj začátek, kde se připravuje na vyšší úroveň dle nových trendů tak, aby odpovídala požadavkům a potřebám svých uživatelů. První fáze zahrnuje výběr dodavatele (v případě, že se jedná o dodavatelský způsob řešení) a to formou výběrového řízení či přímým výběrem (na základě vlastního průzkumu trhu). Ve fázi implementace zase záleží, zda bude postačovat customizace typového software nebo bude třeba vývoj specializovaných nestandardních modulů, součástí této fáze může být i vývoj prototypů. Zakončením této fáze je akceptační řízení, které zahrnuje také testování dílčích částí nebo celku. Po migraci dat následuje organizační příprava zahájení provozu, která je zakončena předávacím řízením, ve kterém je odsouhlasena požadovaná funkcionalita a provozní charakteristiky aplikace. Formálním výstup této fáze je předávací protokol.

Výběr správného typu životního cyklu a odpovídajícího řízení má přímý vliv na výslednou kvalitu informačního systému. Životní cyklus IS může být např. strukturovaný (neboli vodopádový či kaskádový), prototypový (umožňující implementaci a naplnění daty alespoň některých částí IS) či iterativní (krokový, přírůstkový). (Šilerová, 2017) V současné době je patrné zkracování vývojových cyklů, plné využívání mobilních zařízení a postupné využívání smart technologií s prvky IoT (*Internet of Things*). Dynamický trh s ICT produkty a bezprecedentní rychlost rozvoje

ICT favorizují flexibilní inovační procesy a efektivní podnikovou architekturu IS (Basl a Blažíček, 2012). Inovování s sebou přináší značnou konkurenční výhodu pro inovující podniky. *„Životní cyklus informačního systému se neustále zkracuje a stává se, že během rozpracovaného projektu je nutno rozšířit jeho zadání, tzn. inovovat a rozvíjet systém za probíhající implementace. K tomuto jevu dochází zejména ve velkých podnicích, kde zavádění systému trvá déle jak jeden rok.“* (Sodomka a Klčová, 2010)

Inovace, resp. inovování je v životním cyklu podnikového IS stěžejním prvkem. Kontinuální zlepšování a změna informačních systému je prakticky nikdy nekončící proces, který je často reakcí podniku na určité nedostatky. *„ICT inovace jsou i reakcí na zkušenosti se slabými stránkami implementací podnikových IS.“* (Basl, 2011)

Inovace, resp. změny v IS se dle Gála, Poura a Šedivé (2015) povětšinou realizují formou projektů. Změnová řízení se povětšinou vztahují k úpravám funkcionality aplikací. V podniku je třeba mít specifikováno, kdo je oprávněn formulovat požadavky na změny, kde se tyto požadavky evidují, kdo je posuzuje apod. Veškeré navržené změny by měly zapadat do celkové koncepce rozvoje podnikové informatiky. V zásadě existují pouhé dvě možnosti změny dle toho, zda půjde jen o dílčí změnu aplikace, která bude provedena během běžné údržby a nevyžaduje samostatný projekt nebo se již jedná o významnější změnu, zásadní zásah do aplikace, vyžadující specifikaci nového projektu. Tento projekt pak vychází z informační strategie podniku a aktuálních uživatelských požadavků na funkcionalitu a další parametry, které jsou v první fázi předmětem vstupní analýzy, jejímž výsledkem, a tedy podkladem pro specifikaci projektuj je projektový záměr.

Inovační oblasti a typy inovací ICT v podnicích charakterizuje např. Moore (2008), který definuje čtyři oblasti a patnáct typů inovací mající uplatnění v ICT. Základem této typologie je identifikace oblastí inovací reflektujících vývoj trhu – tedy etapy růstu, nasycení a poklesu. Moore identifikuje čtyři oblasti související s vývojem trhu – oblast špičkových produktů, oblast provozní excelence (a oblast důvěrné znalosti zákazníka) a oblast obnovy kategorie.

Tento přístup se do určité míry podobá tzv. hype křivce spol. Gartner, která navíc obsahuje fázi deziluze následovanou stabilizací zájmu. Tato křivka dle Basla (2011) popisuje inovaci z pohledu jejího nasazení a očekávání a následné deziluze z nenaplnění

původních, přespříliš optimistických, očekávání, až po fázi zralosti a užíváním jako produktu – popisuje tedy jakousi zralost adopce technologie. V této souvislosti se rozlišuje několik kategorií inovátorů popisující chování podniků i jednotlivců při osvojování nové technologie, resp. rychlostí její implementace – běžně se tak rozlišuje pět základních skupin – *innovators, early adopters, early majority, late majority, laggards*. Procentuální zastoupení každé z těchto skupin je různé, prakticky sledující trend normálního rozdělení – většinu tvoří early majority a late majority.

Existuje i typologie inovací podle OECD, formulovaná v *Guidelines for Collecting and Interpreting Innovation Data* (Oslo Manual 2018). Ve čtvrtém vydání, ve srovnání s předchozím z roku 2008, došlo k zásadní změně definice podnikové inovace. Z původních čtyř typů inovací (inovace produktu, procesu, organizační a marketingová) došlo k redukci na dva hlavní typy – inovace produktů a inovace podnikových procesů. Inovace produktu je nové nebo vylepšené zboží nebo služba, které se výrazně liší od předchozího zboží nebo služeb firmy a které byly uvedeny na trh. Inovace podnikových procesů je nový nebo vylepšený podnikový proces pro jednu nebo více podnikových funkcí, který se výrazně liší od předchozích podnikových procesů firmy a který firma začala používat.

Inovace, resp. inovační projekty mohou mít podobu například programování (tj. tvorba samotných podnikových aplikací), implementace parametrizovatelného IS (v současnosti dominantní způsob řešení PIS) nebo inovací podnikového IS za účelem zvýšení konkurenceschopnosti podniku např. s využitím teorie omezení (TOC) (Basl a Blažíček, 2012). Při plánování inovací IS je možné postupovat např. v následujících krocích (Koch, 2010):

1. příprava informační strategie firmy,
2. hodnocení přínosů IS/IT,
3. výběr alternativ IS/IT.

2.3.6 Kvalita IS

Kvalitu podnikových informačních systémů ovlivňuje dle Šilerové (2017) celá řada faktorů – např. ekonomická situace podniku, personální zajištění, firemní kultura a klima, schopnosti a možnosti investice do těchto informačních systémů i samotná jejich flexibilita. Nejvíce problematiku flexibility, resp. její absence, řeší častěji spíše

středně velké podniky, právě expandující firmy či podniky s atypickým charakterem podnikatelské činnosti – zvláště tedy podniky ve vysoce konkurenčním prostředí. Kvalita IS/IT je dle Molnára (2001) determinována mírou, jakou informační systémy či technologie přispívají k efektivnosti či výkonnosti procesů v podniku včetně jednotlivých uživatelů. Na IS/IT se tak obecně vztahují stejná hlediska pro posuzování kvality jako na jiné služby či produkty. Za kvalitní tedy považujeme takový systém, který je splňuje dané požadavky nebo je způsobilý k danému užití či účelu. Kvalitu IS předurčuje zvláště jeho funkčnost, spolehlivost, udržitelnost, přizpůsobitelnost, schopnost dalšího rozvoje a zabezpečení. *„Schopnost pracovat s informačním systémem, využívat jej, je ovlivněna právě kvalitou vytvořeného systému“* (Šilerová, 2017).

Při stanovování požadavků je dle autorky nezbytné vycházet ze znalostí uživatelů a jejich schopností a dovedností maximálně využívat funkcionalit informačního systému. Je také důležité definovat požadavky a nároky na uživatelské prostředí, které by mělo být co nejvíce jednotné. Mezi časté nedostatky patří absence zpracování harmonogramu jednotlivých fází životního cyklu informačního systému, jelikož výsledná kvalita systému je ovlivněna zejména počátečními fázemi životního cyklu IS, kdy nezřídka kdy dochází k potížím s implementací.

Kvalita obecně je podrobněji definována např. v základní normě ISO 9000, která definuje systém managementu jakosti. Dle této normy je kvalita produktů a služeb určena „*schopností uspokojovat zákazníky a také zamýšleným a nezamýšleným dopadem na relevantní zainteresované strany*“. Kvalita „*zahrnuje nejen jejich zamýšlenou funkci a výkonnost, ale také jejich vnímanou hodnotu a přínos pro zákazníka*“. (ČSN EN ISO 9000) Mezi konkrétní parametry kvality IS/IT můžeme řadit například: funkčnost, vzhled (resp. komfort), spolehlivost a udržovatelnost, trvanlivost a bezpečnost (Molnár, 2001). Z uživatelského hlediska lze dle autora na kvalitu IS/IT pohlížet z hlediska obsahu, tzn. posuzujeme informace, resp. data podle toho, zda jsou dostatečně přesné, kompletní, zda jsou přiměřeně detailní apod. či z hlediska formy prezentace (zda jsou předávány včas, vhodným způsobem a správným osobám). Pojem kvalita dat, resp. jakost dat se dle Redmana (2008) týká stavu kvalitativních nebo kvantitativních aspektů poskytované informace. Data jsou obecně považována za kvalitní, pokud jsou vhodná k zamýšlené činnosti, rozhodování a plánování.

Výše uvedená uživatelská hlediska jsou dle Molnára (2001) často transformována do podoby technologických ukazatelů, jakými je např. dostupnost (např. doba odezvy), spolehlivost (tj. míra dosažitelnosti a použitelnosti v potřebnou dobu), integrita či bezpečnost. Hodnocení těchto kritérií probíhá nejčastěji buď přímým měřením (je-li to možné) nebo dotazníkovým šetřením. K prověřování kvality IS/IT slouží obvykle audit, jenž má za cíl prověřit především funkčnost, efektivnost a bezpečnost daného řešení. Obvyklými cíli auditu je tedy například zjištění rozporu mezi vyžadovanými a reálně praktikovanými pravidly, zjištění disponibilních zdrojů, zhodnocení informační gramotnosti zaměstnanců nebo nalezení a náprava nejzávažnějších nedostatků, resp. odchylek od obvyklých řešení. Audit může být interní či externí, tedy prováděný (povětšinou nezávislou) poradenskou organizací. Audit by měl začít stanovením cílů a formálních náležitostí následovaných interview s uživateli a výzkumem dokumentů. Posléze by měly být vytipované problémové procesy, na něž se zaměří následné hlubší šetření a posoudí se zjištěné nálezy. Výstupem auditu bývá výrok auditora, zpravidla ve formě závěrečné zprávy o výsledcích auditu.

2.3.7 Efektivnost IS

Podnik by měl mít přehled (a do značné míry i představu) o přínosech, které může zavedením či změnou informačního systému v podniku získat. Podniková informatika buď přispívá k naplňování podnikových cílů a tudíž zjišťujeme, zda je nasazení IS účelné nebo zjišťujeme, jak účinný je samotný IS. (Basl a Blažíček, 2012)

Úvodem je třeba vymezit základní pojmy – efektivitu a efektivnost. Efektivita (*Efficiency*) neboli účinnost je poměr mezi přínosem činnosti a náklady na tuto činnost vynaloženými (Koch, 2010). Jde ji zjednodušeně definovat také jako podíl přínosů a nákladů. Na efektivnost (*Effectiveness*), tj. účelnost, lze obecně nahlížet tak, že u určitého subjektu vznikne potřeba informací a z uspokojení této potřeby plyne jistý užitek. Efektivnost je tedy *„účinnost hodnocená z hlediska užitečného výsledku této činnosti“* (Molnár, 2001).

Efekty podnikové informatiky mohou být vícero druhu, obecně však představují každou pozitivní změnu, tedy přínos, v ekonomických, výkonových, zdrojových či znalostních charakteristikách podniku, vyvolanou užitím informačních technologií (Gála, Pour a Šedivá, 2009). Racionálně se chovající subjekt se dle Molnára (2001)

snaží o hledání vyváženého (tj. optimálního) poměru mezi získaným užitkem z IS/IT a výdaji vynaloženými na dosažení tohoto užitku, ale také potřebným časem a riziky. Na takto vyvážený systém lze pohlížet jako na efektivní. Vložené prostředky jsou v tomto pojetí výdaji na IS/IT, které lze relativně snadno měřit, zatímco přínosy (resp. užitek) lze měřit pouze omezeně, jelikož se projevují nepřímo a se zpožděním (s výjimkami jsou např. systémy podpory pokročilého plánování a rozvrhování výroby APS). *„S rostoucím začleňováním (či přímo splýváním) informačních systémů do procesů firem roste i náročnost odhadu nákladnosti procesů bez zapojení informačních systémů nebo odhad přínosů informačních systémů“* (Koch, 2010).

Z této premisy plynou dva základní přístupy – první je výdajový, kde se soustředíme na náklady spojené s informačním systémem. Je nutné zmínit, že v současné době dochází k posunu paradigmatu od výdajového přístupu k pohledu majetkovému (Basl a Blažíček, 2012). Druhým přístupem je pohled preferující užitek, přínosy a výhody. Nesmíme přitom opomenout fakt, že existuje celé portfolio „příjemců“ užitku – vlastníci podniku, manažeři, zaměstnanci, zákazníci apod. (Molnár, 2011). Vzhledem k faktu, že manažeři či vlastníci podniku nemusí být jediným příjemcem užitku, nejsou ani jediným hodnotitelem aplikací IS v podniku. Implementace PIS totiž musí být v souladu nejen s obecnými podnikovými očekáváními, cíli a procesy, ale je odlišně vnímáno jednotlivými účastníky změn spojených s IS, resp. zainteresovanými stranami (stakeholders), jejichž společným zájmem by měla být dlouhodobá výkonnost firmy. Jednotlivé etapy ovlivňují rozličné skupiny lidí, přičemž jejich vlivy se vzájemně překrývají (Sodomka a Klčová, 2010). Basl a Blažíček (2012) rozlišují čtyři základní stakeholdery a jejich očekávání:

- majitelé – sledují zejména zisk a trvalé zhodnocení svých investic,
- manažeři – očekávají pomoc IS při řízení podniku a dosahování žádoucích efektů,
- zaměstnanci – očekávají zlepšení pracovních podmínek,
- zákazníci – očekávají vhodný produkt za minimální cenu.

Na řízení podnikové informatiky se z ekonomického hlediska můžeme dívat ze svou pohledů – buď je stanoven rozpočet, resp. výše finančních zdrojů alokovaných na informatiku a hledáme jejich efektivní uplatnění, nebo jsou známy požadavky

a hledáme efektivní řešení jejich financování (Šilerová, 2017). Společně s postupným zaváděním informačních systémů a technologií do podnikového prostředí se měnila i očekávání na ně kladená. Dle Molnára (2001) se zpočátku, v 70. letech 20. stol., jednalo o tzv. nahrazovací aplikace, u nichž byly patrné dobře vyčíslitelné přímé přínosy. Později se kromě úspor pracovních sil, materiálu apod. začalo od těchto systémů očekávat i zvýšení přidané hodnoty a hovořilo se o tzv. doplňkových aplikacích, jejichž přínosy byly sice přímé, avšak stále obtížněji vyčíslitelné. Později, od 90. let 20. stol. se začalo hovořit o tzv. inovačních aplikacích, které mají zásadní vliv na klíčové procesy podnikání. Tyto aplikace mají nepřímé a velmi obtížně kvantifikovatelné přínosy. Přínosy je tak možné, i vlivem tohoto vývoje, členit na základní (reprezentované zvyšováním účinnosti a zvyšováním výkonnosti) a inovační (spočívající v podpoře expanze trhu a vytváření konkurenční výhody).

Zkoumání efektivnosti IS/IT lze dle autora postavit na obecném systémovém modelu transformace vstupů na výstupy za působení transformačních faktorů, přičemž je zde snaha o minimalizaci vstupů a maximalizaci výstupů. Ukazuje se, že je nezbytná synergie IS/IT s reengineeringem podnikových procesů. Vazba mezi podnikovými informačními systémy a podnikovými procesy je velmi úzká a de facto koexistenční – nasazení PIS si totiž klade mj. za cíl právě zlepšení podnikových procesů (Basl a Blažíček, 2012). Obecně lze tyto efekty IS/IT kategorizovat na základě obsahové podstaty na (Gála, Pour a Šedivá, 2009):

- finanční výnosy z podnikové informatiky (tržby z produktů a služeb),
- ekonomické efekty informatiky (rozdíly ukazatelů – např. produktivita práce),
- zákaznické efekty (a efekty spojené s pozicí na trhu),
- zvýšení procesní výkonnosti firmy (např. zkrácením doby),
- zvýšení analytické výkonnosti a kvality řízení (podpora rozhodování),
- personální efekty (např. zvyšování kvalifikace).

Finanční výnosy z podnikové informatiky se týkají především informatických společností prodávajících software či poskytujících pronájem technických prostředků. U ostatních firem se může jednat např. o doplňkové informační služby k základním produktům (v případě stavebních či výrobních společností nebo bank), které společnostem přinášejí konkurenční výhodu. Ekonomické efekty jde obecně, vyjma již

zmíněných finančních výnosů, vnímat jako rozdíly v ekonomických ukazatelích způsobených uplatněním určitého informačního systému. Názorným příkladem může být zvýšení produktivity práce nebo nárůst tržeb. Stanovování konkrétních přímých efektů připadajících čistě na zavedení IS je však značně komplikované. Obdobně je na tom i hodnocení přínosů či obecně efektů IS/IT spojených s pozicí podniku na trhu, a proto se využívá také specifických ukazatelů jako jsou ukazatele zákaznické spokojenosti. Podobné „měkké" ukazatele se používají i pro hodnocení personálních efektů, resp. spokojenosti uživatelů. (Gála, Pour a Šedivá, 2009) Pro objektivní hodnocení úspěšnosti projektu je tak vhodné zvolit kombinaci obou kritérií – jak finančních, tak nefinančních, která jsou však v určitém vztahu s kritérii finančními. Nesmíme však opomenout fakt, že efektivnost IS/IT závisí mnohem více na lidech nežli na samotných informačních technologiích, a tudíž je nutné lidské zdroje nejen řídit, ale i motivovat k participaci a kultivovat ve vztahu k informační gramotnosti (Molnár, 2001).

2.4 Ukazatele přínosů IS/IT

Informační systém podniku sám o sobě obvykle žádný ekonomický přínos nepředstavuje (byť existují četné výjimky), kýžených efektů se dosahuje až jeho efektivním využíváním, resp. reálným zhodnocením informací (Šilerová, 2017). Ukazatele přínosů můžeme klasifikovat z celé řady hledisek. Molnár (2001) je dělí na:

- finanční (vyjádřené v peněžních jednotkách) a nefinanční,
- kvantitativní (měřitelné kardinální stupnicí) a kvalitativní (měřitelné ordinálním pořadím či logickou hodnotou),
- přímé (existuje příčinný vztah) a nepřímé (nutné stanovit zástupné ukazatele),
- krátkodobé (projevující se do cca půl roku) a dlouhodobé,
- absolutní a relativní (vyjádřené bezrozměrným poměrovým číslem).

Basl a Blažíček (2012) naopak uspořádávají efekty podnikových IS s využitím metody *Balanced Scorecard* (BSC) a rozlišují následující:

- Finanční efekty,
    - přímé fin. výnosy z informatických produktů a služeb
    - přímé fin. výnosy z inf. produktů a služeb jako z přidané hodnoty k zákl.

        - ekonomické efekty (jako dosažené rozdíly v ekonomických ukazatelích vlivem ICT
- Zákaznické efekty,
    - efekty spojené s pozicí na trhu (podíl na trhu apod.)
- Procesní efekty,
    - efekty spojené s procesní výkonností (zkrácení průměrné doby zakázek apod.)
    - zvýšení kvality řízení a úrovně komunikace v podniku
    - zvyšování výkonnosti procesů na základě jejich monitorování
- Učení a růst,
    - efekty způsobené zmapováním znalostí uživatelů (vč. aplikace principů Knowledge Managementu)
    - zvyšování kvalifikační úrovně zaměstnanců.

Hodnocení přínosů IS/I (C)T je nezbytnou součástí posuzování informačních systémů v podnicích. Nefinanční měřítka však nejsou standardizována a pro objektivní zhodnocení přínosů IS/IT v podniku je vhodné zvolit vyváženou kombinaci obou ukazatelů, tj. jak finančních, tak nefinančních kritérií (Šilerová, 2017). Možnosti použitelných ukazatelů se liší napříč podniky a neexistuje jednotná sada či systém ukazatelů, které by bylo možné mechanicky aplikovat na každý podnik. Někteří autoři, např. Laudon a Laudon (2005) doporučují hodnotit samostatně investice do technologií (infrastruktury) a investice do aplikací informačních systémů. Obecně však lze konstatovat, že u všech ukazatelů musíme sledovat hledisko účelnosti, která je vyjádřena obecně měřitelnou mírou dosažení cílů. Jako finanční ukazatele přínosů IS/IT se většinou používají standardní ukazatele efektivnosti investic (Molnár, 2001). Pro hodnocení ekonomické efektivnosti investičních projektů se nejčastěji používá rentabilita kapitálu (celkového či vlastního), doba návratnosti nebo kritéria založená na diskontovaném cash flow (čistá současná hodnota – NPV, index rentability – PI a vnitřní výnosové procento – IRR) (Fotr a Souček, 2011; Basl a Blažíček, 2012). Dalšími použitelnými metodami může být například *Total Cost of Ownership* – TCO (ten je vhodný zejm. při potřebě porovnání nabídek více dodavatelů, popř. posuzování již existujícího IS a jeho benchmarking), ROI, TVO, BSC či EVA. Ukazatel TCO však nekalkuluje s přínosy IS/IT a často se u něho opomínají nepřímé náklady (spojené např.

s výpadky či neformálním učením uživatelů), což vede ke zkreslování výsledků (Koch, 2010). Větší důraz na hodnocení efektů PIS směrem k jejich business přínosům je kladen v přístupu označovaném Val IT (Value IT), používaného spíše v zahraničí. Ten představuje rámec zahrnující principy klíčových manažerských praktik a vychází z metodiky COBIT. (Basl a Blažíček, 2012) *„Ekonomické přínosy různých SW produktů a aplikací byly v našich průmyslových podnicích donedávna formulovány a vykazovány spíše nepřímo – úspora lidských zdrojů, zrychlení práce s informacemi, zlepšení informovanosti vedoucích pracovníků“* (Šilerová, 2017).

Nefinanční kritéria musí splňovat tři základní podmínky – musí umět rozlišovat dobré a špatné, musí být kontrolovatelná (a měřitelná), aby se dala hodnotit a zlepšovat, a musí zajistit vztah mezi nefinančním a finančním úspěchem, který se však obtížně prokazuje, jelikož se projevuje až po delší době a je špatně průkazný (Šilerová, 2017). Lze však obecně říci, že správné informace v kombinaci se zlepšenými podnikovými procesy, vhodnou podnikovou kulturou a informačně gramotnými zaměstnanci snižují náklady a mohou zvyšovat výnosy (Basl a Blažíček, 2012). Mezi nefinanční, avšak měřitelné ukazatele přínosů IS/IT se řadí zejména produktivita, která poskytuje údaje o vztahu mezi vstupními náklady a výstupním užitkem, resp. poměru mezi množstvím vstupů a množstvím výstupů za určitý čas. Informační systémy se podílí na zvyšování efektivity efektivnějším využíváním podnikových zdrojů. Mezi měřitelné ukazatele se řadí i nejrůznější doby (např. doba výroby), počty (např. reklamací) nebo podíly (např. ve specifickém segmentu trhu). Výrazným ekonomickým efektem zavádění IS/IT je povětšinou také úspora pracovních sil, přičemž se podstatně mění pracovní náplň jednotlivých zaměstnanců podniku (Šilerová, 2017). Jak uvádí Molnár (2001), takřka všechny měřitelné ukazatele se dají převést na ukazatele finanční, vyžaduje to však přesné statistické údaje nebo užití kvalifikovaného odhadu. V případě použití tzv. „měkkých“ ukazatelů je vhodné najít zástupné „tvrdé“ ukazatele, které budou co nejlépe reflektovat jejich změnu. Mezi měkké ukazatele se řadí zejména ukazatele spokojenosti (zákazníků, zaměstnanců), které lze kvantifikovat určitými indexy, nebo také kvalita pracovního prostředí (měřena průzkumy a zástupně vyjádřena např. fluktuací zaměstnanců) apod.

2.4.1 Výdaje na IS/IT

Za účelem kvantifikace efektů IS/IT má smysl porovnávat nikoliv absolutní výdaje na IS/IT, nýbrž poměrové ukazatele (např. roční výdaje jako procento z celkového ročního obratu nebo výdajů), pomocí kterých můžeme porovnávat útvary či podniky mezi sebou a sledovat také jejich vývoj v čase. Výdaje na IS/IT můžeme obecně klasifikovat dle tří hledisek (Molnár, 2001; Šilerová, 2017):

- časové hledisko (dle životních fází),
- druhové hledisko (např. HW, SW, implementace, údržba),
- aplikační hledisko (dle aplikací, je-li možné k nim přiřadit přínosy).

Dle Šilerové (2017) je při klasifikaci dle časového hlediska nutné kalkulovat s celým životním cyklem IS/ICT, tj. celou dobou životnosti systému. Velmi rychlý rozvoj IS/ICT, zvyšující se požadavky i objemy dat vedou ke zkracování životnosti systémů zejm. vlivem morálního zastarávání. Z časového hlediska se výdaje dále rozlišují na jednorázové výdaje, běžné (provozní) výdaje a skryté výdaje (tj. náklady nepřiřazené k celkovým nákladům spjatým s provozem IS, ale účtované k nákladovému středisku). Čím vyšší jsou skryté výdaje, tím méně věrohodně jsou ekonomické ukazatele. Z druhového hlediska lze výdaje na IS/IT členit dle nákladových položek spjatých s provozem – např. na hardware, software, lidské zdroje, služby externích dodavatelů (servis, údržba) či režii útvarů pro IS/ICT. Zejména sledování těchto druhově členěných výdajů má vliv na efektivní vynakládání zdrojů na IS/ICT v organizaci, potažmo na celkové hospodaření podniku. Z aplikačního hlediska členíme výdaje na výdaje spjaté např. s informačními systémy, s aplikacemi Business Intelligence, s komunikačními aplikacemi, kancelářskými aplikacemi, popř. lze vyjádřit výdaje dle jednotlivých agend či modulů (např. účetnictví, skladové hospodářství apod.). Tato výše zmíněná hlediska lze dle potřeby účelově kombinovat, čímž se mohou stát základním controllingovým hlediskem při sledování výdajů na podnikovou informatiku (Molnár, 2001).

2.5 Procesy

Procesy jsou definovány jako „*vzájemně provázané činnosti, které přeměňují vstupy na výstupy*“ (ČSN EN ISO 9000). Procesy lze dle Gály, Poura a Šedivé (2015) dělit na základní (či klíčové) procesy, kterými jsou zajišťovány hlavní podnikové funkce

bezprostředně spojené s uspokojováním potřeb zákazníků a podpůrné procesy, které probíhají uvnitř podniku a mají pouze podpůrný charakter. Tyto se mohou dále dělit na procesy podpůrné služební (specializované na určitý produkt) a podpůrné průřezové (sloužící mnoha okolním procesům). Basl a Blažíček (2012) uvádějí ještě procesy vedlejší, což jsou procesy určené pro vnitřního zákazníka, které je možné outsourcovat bez ohrožení strategie. Někdy se také v literatuře uvádí třetí, nejnižší, kategorie procesů, a to procesy pomocné. Z pohledu vlastníka lze procesy dělit na interní, jež jsou plně pod kontrolou managementu podniku a externí (Sodomka a Klčová, 2010). U externích procesů není vlastník přesně definovaný, a tudíž řízení těchto procesů nemá podnik plně pod kontrolou. Sodomka a Klčová (2010) dále kategorizují procesy na řídící (např. řízení kvality a strategické plánování), hlavní (hodnototvorné) a podpůrné (nejsou součástí hodnototvorného řetězce). „*Z hlediska nasazení podnikových IS je důležité dělení procesů podle jejich automatizovatelnosti, protože IS jsou využitelné zejména pro podporu dobře automatizovatelných procesů*“ (Basl a Blažíček, 2012).

V praxi se používá také metodika *Capability Maturity Model* (CMM), která dělí procesy dle stupně jejich zralosti (Basl a Blažíček, 2012):

- neexistující – není pozorovatelný, při výskytu události spontánní reakce,
- náhodný – ad hoc řešení, neexistuje konsolidovaný přístup,
- opakovaný, ale pouze intuitivní – existuje snaha o standardizaci,
- formalizovaný – standardizace a popis procedur, ale realizace na jednotlivcích,
- měřitelný – přidán proces řízení a kontroly průběhů, neustále zlepšování,
- optimalizovaný – nejlepší stav, činnosti zaměřené na optimalizaci jsou již součástí procesu.

Proces má několik základních charakteristik – je opakovatelný (pokud je standardizován), je měřitelný určitými parametry (např. KPI), jeho výstupem je statek s přidanou hodnotou, má svého vlastníka (který má nad ním kontrolu a je za něho odpovědný), má svého zákazníka (interního nebo externího) a je jasně vymezen jeho začátek, jeho konec a jeho návaznost na další procesy (Sodomka a Klčová, 2010). Procesy je tedy možno definovat, měřit a zlepšovat. Zlepšování procesů v podniku začíná již před samotnou implementací informačního systému, kdy probíhá jejich mapování a vytváří se model současného stavu procesů, který slouží jako podklad pro

implementaci IS, ale také k úpravám samotných procesů. Identifikují se například slabá místa procesů, probíhají úvahy o outsourcingu apod. (Basl a Blažíček, 2012) Analýzou vnitropodnikových procesů a konfrontováním jejich podílu na plnění stanovených cílů se stavem jejich zabezpečení ze strany IS/IT se zabývá například metoda *Process Quality Management* (PQM), při které se určují konkretizované tzv. kritické faktory úspěchu (CSF) nebo analýza hodnotových řetězců (*Value Chain Analysis*, VCA), pomocí níž hledáme, jak a kde se v podniku tvoří hodnota pro zákazníka. (Molnár, 2001)

2.5.1 Procesní modelování

Při vytváření zcela nově definovaných procesů, ale i při modifikování stávajících procesů se dle Gály, Poura a Šedivé (2015) může uplatnit procesní modelování. Souhrnně se tato činnost označuje jako *Business Process Reengineering* (BPR). Aby bylo možné procesy kontinuálně zlepšovat, je nutné je nejprve zdokumentovat. Do dokumentace patří detailní charakteristika vstupní události, popis jednotlivých činností (s použitím logických operátorů), vstupy a výstupy, role (RACI matice – *responsible, accountable, consulted, informed*), metriky a popř. softwarové nástroje, které proces zajišťují či podporují. Průběh určitého procesu je možné znázornit například pomocí EPC diagramu (*Event-driven Process Chain*).

2.6 Strategie implementace IS

Potřebujeme-li nahradit stávající informační systém (nebo jeho část) systémem novým, popř. zavést do podniku zcela nový informační systém, je třeba k tomu zvolit vhodnou strategii. K vizualizaci postupových kroků v rámci implementace IS je možné použít tzv. Ganttovy diagramy. Koch (2010) rozlišuje několik základních strategií implementace IS:

- souběžná strategie – tj. provozování obou systémů po určitou dobu,
- pilotní strategie – zavedení nového IS nejprve v jedné pobočce/oddělení,
- postupná strategie – postupné odebírání částí starého IS a nahraz. novým IS,
- nárazová strategie – ukončení a nahrazení IS.

Autor dále uvádí, že souběžná strategie spočívá v překrývání obou systémů, zatímco dochází o ověření funkčnosti systému (např. betatestování) a přeškolení pracovníků. Jedná se o relativně bezpečnou, nicméně nákladnou a pracnou strategii implementace. Pilotní strategie zahrnuje odzkoušení nového IS v jedné části podniku a postupný přechod i na zbytek organizace. Tato strategie je relativně bezpečná, ovšem náročná na koordinaci a vzájemnou kompatibilitu dat a úloh obou systémů. Postupná strategie je oproti předchozím výrazně pomalejší, nicméně bezpečná. Tento typ je používán zejména pro inovaci rozsáhlých informačních systémů. Nejriskantnější, nicméně nejrychlejší je strategie nárazová, kdy se starý systém ukončí, aby byl posléze ihned nahrazen systémem novým. *„Zavádění informačních systémů je velmi složitý proces, charakterizovaný prosazováním mnoha často protichůdných požadavků, obtížnou řiditelností nesourodého týmu lidí (konzultanti dodavatelské firmy, programátoři, klíčoví uživatelé, manažeři) s různými vlastnostmi a schopnostmi"* (Sodomka a Klčová, 2010). *„Z praxe jsou známy příklady, kdy i dobře navržené informační systémy postavené na posledních technologických poznatcích ztratily v důsledku nezvládnuté implementace většinu své užitné hodnoty*" (Basl a Blažíček, 2012).

2.7 Způsob pořízení a možnosti rozvoje IS

Před managementem podniku obvykle stojí rozhodnutí, zda zvolit nákup hotového informačního systému, nechat si vyvinout IS na míru (popř. si ho vyvinout vlastní činností) nebo zvolit pronájem IS. Při rozhodování hraje roli celá řada kritérií. Hotové IS jsou k dispozici relativně rychle a levně, avšak nabízí omezené možnosti customizace. V případě obvykle dražšího vývoje je zde naopak vyšší závislost na dodavateli apod. (Koch, 2010). V praxi je třeba důsledně zanalyzovat potřeby dané konkrétní společnosti a nadefinovat přesné požadavky na informační systém, který je třeba správně nadesignovat (tj. vybrat aplikaci, framework atp.), přičemž pro samotný vývoj IS/SW existuje celá řada různých přístupů. *„Vývoj zcela nového systému na zakázku lze použít především u malých, relativně izolovaných částí IS a v malých firmách. Ve větších firmách je zřetelně vidět příklon k integrovaným řešením (ERP), kde vývoj zcela nové aplikace bývá jednoznačně nahrazován nákupem hotového systému."* (Koch, 2010)

Existuje tedy několik různých přístupů k řešení IT aplikací, přičemž se mohou v rámci daného aplikačního portfolia různě kombinovat. Dle způsobu pořízení se obecně rozlišují (Gála, Pour a Šedivá, 2015):

- aplikace vyvinuté externí společností – outsourcing vývoje (typické u ERP, CRM apod.),
- aplikace vyvinuté zaměstnanci podniku – zajišťující specifickou, unikátní funkcionalitu, popř. bezpečnostně citlivé realizace nebo naopak relativně jednoduché dashboardy v prostředí BI.

Podle možnosti, resp. nutnosti modifikování se dle autorů rozlišují na:

- aplikace typové (*Commercial Off The Shelf*, COTS) – předpokládá se použití v různých podnicích, popř. odvětvích,
- aplikace jednoúčelové – vytvořené dle specifických potřeb podniku tam, kde není možné využít typizované řešení, popř tam, kde usilují o dosažení konkurenční výhody.

Aplikace lze dále dle autorů členit například dle provázanosti (aplikace spojené do balíku aplikací vs. aplikace se slabou, na standardech založenou, vazbou na ostatní aplikace), dle míry možného zasahování do aplikace (black box, gray box, white box) či související míry otevřenosti zdrojového kódu aplikace (open source software – svobodné užívání a modifikace, proprietární software – licence upravena EULA).

Řízení podnikové informatiky tvoří podstatnou část řízení celého podniku, jelikož informatika zasahuje prakticky do celé struktury firmy a jsou kladeny čím dál tím vyšší požadavky na dostupnost informačních zdrojů. Rozvoj podnikové informatiky se dle Gály, Poura a Šedivé (2015) realizuje na základě projektů, úzce tedy souvisí s projektovým řízením, resp. řízením projektů ve sféře IT. Řízení projektů IS/ICT se týká jak hardware (např. instalaci nových technologií), tak software (implementace nových aplikací), v praxi však často dochází k souběžné kombinaci obojího. Provoz podnikové informatiky sestává z celé řady činností, zmínit lze např. zajišťování provozu celé počítačové sítě, monitoring provozu, řešení poruch, nastavování přístupových práv, instalace HW i SW, správa databází, analýza logů, zajištění helpdesku, evidence problémů atd.

2.7.1 Outsourcing

Outsourcing v (podnikové) informatice je zajišťování vybraných činností a služeb externími dodavateli a je možné jej dále členit na outsourcing rozvoje a outsourcing provozu, který nabývá na významu společně s využíváním služeb Cloud Computingu (Gála, Pour a Šedivá, 2015). Šilerová (2017) popisuje dva specifické typy outsourcingu v oblasti IS/IT – outsourcing vývoje informačního systému, popř. dodání customizovaného již hotového řešení či outsourcing provozu – ten je již v pravém slova smyslu outsourcingem, jelikož ICT jsou majetkem dodavatele/poskytovatele, systém je u něho umístěn a je jím spravován, a jsou u něho obvykle také uložená veškerá data. Koch (2010) toto řešení, tedy podmnožinu outsourcingu zaměřenou na poskytování aplikačních služeb IS/ICT označuje jako ASP (*Aplication Service Providing*). Je nutné podotknout, že by se vždy mělo jednat o dodávku služby, a to opakovaně a trvale (Molnár, 2001). Hlavním předmětem uvažování, mluvíme-li o outsourcingu, jsou tedy zejména úvahy co vytěsnit, učinit rozhodnutí, zda to vytěsnit, stanovit finanční efekty vytěsnění, kalkulovat s konkurenční výhodou vytěsnění (zejm. možností větší specializace na hlavní činnost) a uvažovat nad dlouhodobými důsledky samotného vytěsnění (Šilerová, 2017). Plánování outsourcingu, tj. obstarávání či nakupování, je obvykle důsledkem provádění analýz make-or-buy, tedy analýz, zda má z nákladového hlediska smysl si produkt či službu zajistit vlastními silami nebo jej obstarat, tzn. nakoupit z vnějších zdrojů. *„Objem outsourcingu v oblasti informačních technologií roste, a to jak v soukromém, tak státním sektoru. Outsourcing organizacím umožňuje snížit si náklady, soustředit se na jádro svého podnikání, dostat se ke specifickým dovednostem a technologiím, být flexibilnější a přenést větší zodpovědnost na dodavatele.“* (Schwalbe, 2011)

Důvody pro outsourcing jsou různé – může jimi být úspora nákladů, nedostatek odborných znalostí či časových možností. Podniky si od outsourcingu slibují získání konkurenční výhody, zdokonalení v oblasti hlavního předmětu podnikání, jelikož část (zpravidla podpůrných) činností odpadne, což umožňuje vyšší specializaci, dále snížení nákladů (zvláště v krátkodobém horizontu), a v neposlední řadě i zjednodušení organizační struktury podniku (např. typicky u outsourcingu IT) (Šilerová, 2017). Outsourcing s sebou přináší zvýšení flexibility a rychlejší uplatnění nových technologií, avšak nese také určitá rizika, mezi něž patří např. závislost na dodavateli nebo

bezpečnostní rizika, resp. vyšší nároky na informační bezpečnost (Gála, Pour a Šedivá, 2015). Toto řešení s sebou nese také určitou ztrátu kontroly nad aplikacemi a jejich kvalitou (Koch, 2010). Molnár (2001) navíc ještě upozorňuje na diametrálně rozdílnou maximální velikost odpovědnosti za škodu u zaměstnance v porovnáním se smluvní odpovědností externího partnera a určitou nevratnost strategického rozhodnutí. Dalším zřejmým rizikem je problematika bezpečnost informací, kdy sdělujeme citlivá data třetímu subjektu, ale také úzká provázanost s organizací. Prostor pro eliminaci těchto rizik plyne dle Šilerové (2017) z obchodního vztahu mezi zákazníkem a poskytovatelem a v praxi má obvykle charakter smlouvy o poskytování služeb.

Význam outsourcingu v podnicích nabývá společně s rozvojem komunikačních technologií – např. IT podpora se může vzdáleně připojit na pracovní stanici uživatele a nevyžaduje to jeho fyzickou přítomnost na pracovišti. Rozvoji outsourcingu tedy nahrává extrémně rychlý vývoj technologií, na který reagují specializovaní poskytovatelé outsourcingových služeb zpravidla rychleji a jsou tedy schopni poskytovat lepší služby. Outsourcing je tedy velmi vhodným řešením v případě, kdy zabezpečujeme „standardní“ procesy probíhající u velké většiny organizací – např. vedení účetnictví či kancelářské aplikace, kdy nám funkčnosti těchto systémů do značné míry určuje dodavatel (s respektováním odlišností dle segmentu podnikání – tzv. branchová řešení) a tak si zde spolu s informačním systémem podnik většinou kupuje i know-how „optimálního“ systému řízení daných procesů (Molnár, 2001). V závislosti na způsobu pořízení můžeme také uvažovat s různým způsobem financování, které může být buď z vlastních zdrojů, nebo může podnik použít zdroje cizí (Režňáková, 2012). Koch (2010) však připomíná, že existují oblasti IS/ICT, ve kterých se outsourcing aplikačních služeb IS/ICT, resp. model ASP nejeví jako vhodný. Jedná se například o:

- Mission Critical Core Business Applications neboli unikátní aplikace, na kterých je založen hlavní předmět podnikání firmy,
- vysoce specializované a customizované aplikace,
- aplikace s vysokými nároky na integraci s ostatními podnikovými aplikacemi.

2.8 Metodiky a modely řízení podnikové informatiky

Pro řízení podnikového informatiky existuje celá řada metodik, konceptů, standardů, modelů a frameworků, jejichž účelem je zkvalitnění jejího řízení, resp. snižování nákladů na ni, lepšímu zhodnocování realizovaných investic a dosahování kýžených efektů. Řadí se mezi ně např. CMMI (hodnocení zralosti a úrovně řízení), ISO/IEC 12207 (inovace ve vývoji a životním cyklu SW), ISO/IEC 15504 (posuzování a auditing) ad. (Basl, 2011). Na nižších úrovních podnikové informatiky můžeme identifikovat efekty jejího řízení například pomocí metod ITIL a COBIT (Basl a Blažíček, 2012). Oba tyto přístupy, tj. jak ITIL, tak COBIT, představují dle Kocha (2010) současný trend v řízení IS/IT. Společný jim je i procesní pohled, což je dáno mj. tím, že ITIL při svém vzniku čerpal z COBIT. Není zde však plný obsahový soulad a metodika ITIL je navíc snáze pochopitelnější a značně přehlednější. Zavádění standardů a norem, zvláště pak v oblasti IS/IT, je však značně náročné na zdroje, tudíž zavádění těchto metodik realizují spíše větší organizace (Basl, 2011).

2.8.1 ITIL

IT Infrastructure Library (ITIL) je rámec skládající se ze sady vzájemně provázaných publikací, které popisují best practices při řízení informatiky organizace (Basl a Blažíček, 2012). Certifikace ITIL je dostupná pouze pro jednotlivce a v současnosti je nejnovější verzí ITIL V4 (vydán v roce 2019), která se skládá ze dvou klíčových komponent – čtyřdimenzionálního modelu a hodnotového systému služeb. (Gála, Pour a Šedivá, 2015) Na službu ITIL nahlíží ze dvou hledisek – z pohledu koncového uživatele a z pohledu jejího životního cyklu (Koch, 2010). Model definuje čtyři dimenze, které by měly být zohledněny, aby byl zajištěn holistický přístup k řízení služeb: Organizace a lidé, Informace a technologie, Partneři a dodavatelé, Toky hodnot a procesy. K hlavním efektům implementace metodiky ITIL v praxi tak patří kontinuální zlepšování procesů a zvyšování jejich efektivity, jedná se však o složitý a zdlouhavý proces. (Gála, Pour a Šedivá, 2015)

2.8.2 COBIT

Control Objectives for Information and Related Technology (COBIT) je model skládající se procesů a metrik jejich efektivnosti, který je v souladu např. s ITIL, Prince2, ISO nebo COSO (Basl a Blažíček, 2012). COBIT slouží ke zlepšování procesů v pěti základních oblastech (Gála, Pour a Šedivá, 2015):

- vazba strategií – provázání podnikatelských plánů s plány podnikové informatiky,
- dodávka hodnoty – přidané hodnoty prostřednictvím informatiky,
- řízení zdrojů – optimalizace investic (IT, HR),
- řízení rizika,
- měření výkonnosti – kontrola hospodárnosti.

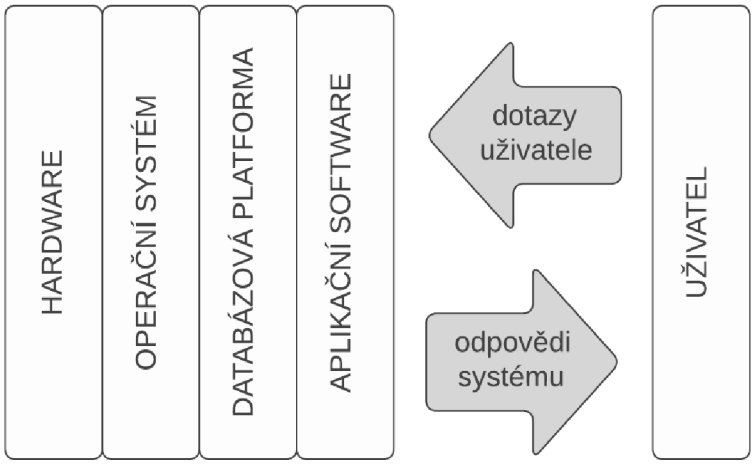
V oblasti IT Governance, tedy metodiky řízení je v současné době COBIT standardem, jelikož definuje zralostní modely, cíle a míry a cíle činnosti umožňující řídit procesy (Basl, 2011). Dle Basla a Blažíčka (2012) obsahuje COBIT komplexní systém cílů a metrik (vč. měkkých), který reprezentuje ucelený a schematický pohled na řízení podnikové informatiky a je ho možné využít pro provádění auditů. V tomto modelu je podniková informatika rozdělena dle funkčních domén (PO, DS, AI, ME), informačních kritérií a vztah mezi těmito entitami je výsledně přiřazen zdrojům. V rámci tohoto modelu je dále pro každý jednotlivý proces vymezen tzv. model zralosti (Maturity Model) obsahující konkrétní kritéria a metodu hodnocení provádění kontroly kvality procesu, přičemž hodnotící škála zvládnutí procesu je pro všechny podnikové procesy společná. Dochází tedy ke komplexnímu a normovanému náhledu na způsob řízení IS/IT v podniku.

2.9 Klasifikace podnikových IS

Informační systémy, resp. aplikace podnikových IS, lze členit z celé řady pohledů – např. z pohledu architektur, úrovně řízení, okolí či odbytu výroby. Každá organizace se skládá z několika organizačních úrovní, z nichž každá požaduje specifický druh či způsob zpracování informací (Sodomka a Klčová, 2010). Nejčastěji se v literatuře lze setkat s rozlišením strategické, řídící, znalostní a provozní úrovně (Laudon a Laudon, 2005). Dle Sodomky a Klčové (2010) nemůže žádná z těchto úrovní individuálně

poskytnout všechny informace potřebné pro řízení, stejně jako nepředstavuje ucelenou entitu, která by vyžadovala, resp. reflektovala potřebu, nasazení samostatného informačního systému či softwarové aplikace. Tato klasifikace tedy reflektuje teoretický koncept fungování podniku, jelikož charakterizuje hodnotu automatizovaného zpracování informací pro pracovníky na jednotlivých dílčích úrovních organizace. Do provozní úrovně spadá zpracování informací týkajících se rutinní podnikové agendy, jako je například zpracování mezd nebo příjem objednávek. S touto úrovní se pojí zejména transakční systémy. Znalostní úroveň již zahrnuje nejen klientské aplikace, ale také tzv. prostředky osobní informatiky, což jsou kancelářské aplikace, komunikační aplikace nebo groupware. Řídící úroveň vyžaduje informace k podpoře rozhodování – na této úrovni jsou výstupy pro uživatele často formou reportů či analýz. Nejvyšší, strategická úroveň, zahrnuje systémy sloužící mj. k identifikaci dlouhodobých trendů, které často agregují informace nejen zevnitř, ale i ze vně podniku.

Dalším ze způsobů, jak můžeme dle autorů na podnikové informační systémy nahlížet, je tzv. technologický pohled, který má blíže k praxi. Jedná se o rozdělení na bázi vrstev, jež dohromady tvoří komplexní systém a jimiž, nebo skrze které, jsou data transformována v informace. Z tohoto pojetí zřetelně vyplývá, že hardwarová a softwarová infrastruktura zajišťující efektivní automatizované zpracování dat je nedílnou součástí podnikového IS.



Obrázek č. 7: Technologické pojetí informačního systému
(Zdroj: vlastní zpracování dle Sodomky a Klčové, 2010)

Relativně častý je také tzv. holisticko-procesní model, jenž klasifikuje podnikové IS dle jejich praktického uplatnění v podniku, ve shodě s požadavky na řízení procesů a nabídkou dodavatelů. Dílčí součásti IS poskytuje prostředky systémová integrace. Dle Sodomky a Klčové (2010) se podnikový IS podle tohoto způsobu klasifikace skládá z:

1. ERP jádra, zaměřeného na řízení interních procesů,
2. CRM systému podporujícího procesy směrem k zákazníkům,
3. SCM systému na řízení dodavatelského řetězce (obvykle včetně APS systému),
4. MIS, které sbírá data z výše uvedených systémů a externích zdrojů.

Gála, Pour a Šedivá (2015) uvádí, že pro tyto podnikové systémy je příznačná jejich vysoká heterogenita, jelikož aplikace nabývají vlastností z celé řady hledisek – např. kterým uživatelům jsou určeny, jaká data využívají, jaká je jejich funkcionalita, jaké podnikové procesy či oblasti řízení podporují a na jakých technologiích jsou tyto aplikace provozovány. Všechny tyto aplikace však mají společnou vlastnost, že poskytují určité funkce svým uživatelům a manipulují daty s využitím software, hardware a lidí. Souhrn všech aplikací podniku tvoří tzv. aplikační portfolio.

V současnosti prakticky veškeré podniky používají nějakou formu software pro ukládání a zpracování podnikových dat. Rozsáhlost tohoto činění je pochopitelně závislá na velikosti firmy, předmětu jejího podnikání a množství zpracovávaných dat, schopnostech jejich zaměstnanců apod. Malé firmy používají dle Šilerové (2017) zejména ekonomické a účetní moduly určené pro práci s firemním účetnictvím, lidskými zdroji, sklady apod. Integrace těchto modulů je často omezená a data se mnohdy musejí předávat zásahem uživatele. Analytické nástroje jsou povětšinou omezeny na tabulkové procesory (MS Excel). Střední podniky již používají software s větším analytickým rozsahem, jedná se často o komplexní ekonomický software s dobře integrovanými moduly. Velké společnosti používají typicky SW pro plánování a řízení většiny procesů ve firmách – tedy již zmíněné ERP systémy.

Tyto systémy jsou zaměřené na podporu transakcí, resp. se jedná o aplikace pro řízení podnikových zdrojů (*Enterprise Resource Planning*, ERP). Tyto aplikace jsou často používané zejména u podniků výrobního či obchodního charakteru a svým uživatelům umožňují mj. vytváření rozsáhlých databází, zpracování obchodních operací atp. (Gála, Pour a Šedivá, 2015). Aplikace pokrývají prakticky veškeré základní oblasti

podnikového řízení – nákup, prodej, skladové hospodářství, finanční účetnictví, controlling, HR, plánování výroby atp. Neexistuje jednotná definice ERP systému – některé z nich na něho hledí z pohledu datového, jiné straní funkčnímu a další zase procesnímu pohledu. Některé definice navíc zdůrazňují význam automatizovatelnosti dané oblasti, což lze ilustrovat na příkladech přínosů ERP systémů při automatizaci účetnictví, skladování či plánování (Basl a Blažíček, 2012). Mezi základní požadavky na ERP systémy patří plná integrace, práce v reálném čase, jednotné uživatelské rozhraní napříč moduly (zajišťující intuitivní ovládání uživateli) a jednotná databáze (popř. jejich propojení) (Šilerová, 2017). Sodomka a Klčová (2010) ERP systémy klasifikují podle oborového a funkčního zaměření na All-in-One, Best-of-Breed a Lite ERP.

Tyto systémy jsou často již vytvořené dodavateli a jsou následně přizpůsobovány na míru danému podniku. Při implementaci ERP se však může vyskytnout celá řada problémů, od narušení podnikových procesů, problematické integrace dat, až po ústupky v některých oblastech při implementaci systému na celou firmu. ERP systémy často představují základní východisko a jsou spojeny s dalšími aplikacemi např. na řízení výroby (*Manufacturing Execution System*, MES), aplikacemi automatizace skladů (*Warehouse Management System*, WMS), plánovacími systémy (*Advanced Planning and Scheduling*, APS) nebo aplikacemi na řízení životního cyklu podniku (*Product Lifecycle Management*, PLM) (Gála, Pour a Šedivá, 2015).

Nedílnou součástí podnikového IS jsou aplikace mající tzv. infrastrukturní charakter, tj. nejsou přímo spojeny s určitými podnikovými procesy nebo oblastmi řízení, což znamená, že jsou využívány napříč celým IS. Mezi aplikace infrastrukturního charakteru patří například aplikace pro správu dokumentů, řízení pracovních toků, portálová řešení apod. Tyto aplikace se souhrnně označují jako *Enterprise Content Management* (ECM) neboli správa podnikového obsahu. (Sodomka a Klčová, 2010; Gála, Pour a Blažíček 2015)

Dále dle autorů existují také aplikace podporující řízení řízení externích vztahů podniku, sem patří například systémy řízení dodavatelských řetězců (*Supply Chain Management*, SCM), popř. analogicky ve vztahu k zákazníkům *Demand Chain Management* (DCM), systémy řízení vztahů se zákazníkem (*Customer Relation*

Management, CRM; a dílčí systémy SFA, EMA nebo CSS), aplikace konkurenčního zpravodajství (*Competitive Intelligence*, CI) nebo aplikace pro podporu rozhodování (*Business Intelligence*, BI). Vedle těchto kategorií existují i aplikace pro podporu produktivity zaměstnanců, což jsou například nejrůznější kancelářské či komunikační aplikace. Kancelářské informační systémy (*Office Information Systems*, OIS) dle Šilerové (2017) slouží jako podpůrné nástroje pro všechny úrovně řízení v podniku. Kancelářské IS usnadňují komunikaci i činnosti jednotlivých týmů, správu dokumentů apod. Tyto aplikace umožňují efektivnější řízení workflow a vytvářejí prostředí pro nastavení lepších procesů v podniku, ať už se jedná o každodenní administrativní agendu nebo kolaboraci napříč týmy.

2.9.1 Enterprise Content Management

„*Enterprise content management (ECM) jsou aplikace a technologie, které poskytují prostředky pro vytváření, sběr, správu, zabezpečení, ukládání, uchovávání, likvidaci, publikování, distribuci, prohledávání, personalizaci a prezentaci, prohlížení, tisk veškerého obsahu podniku*“ (Gála, Pour a Šedivá, 2015). Obsahem podniku se zde myslí veškerá nestrukturovaná a částečně strukturovaná data, která se v organizaci nacházejí (Kunstová, 2009). Nezáleží přitom na jejich formě, může se jednat jak o informace v listinné podobě, tak data v elektronické podobě. Základní jednotkou dat, resp. základním celkem, je zde dokument, což je, dle zákona o archivnictví „*každý písemný, obrazový, zvukový, elektronický nebo jiný záznam*“ (Zákon č. 499/2004 Sb.). Dokumenty procházejí životním cyklem, od svého vzniku (pořízení, přenesení či digitalizací), přes zpracování a uchovávání (archivaci), až po jeho zánik (skartací či výmazem). Poté, co jsou dokumenty digitalizovány a informace v nich obsažené vytěženy, je nutné řešit správu dokumentů, aby bylo možné řídit jejich organizaci, změny apod. Systémy řešící správu dokumentů se označují *Document Management System* (DMS). Systémy ECM také podporují týmovou spolupráci (kooperaci, kolaboraci), komunikaci mezi zaměstnanci, automatizaci workflow či interních procesů nebo správu znalostí (*Knowledge Management*).

2.9.2 Document Management System

Technologie *Document Management System* umožňují sdílení dat, verzování spravovaných dokumentů, kolaboraci více uživatelů současně (vč. modifikace), práci s metadaty a tagy, vyhledávání (vč. obsahu) a řídit pravidla bezpečnosti (řízení přístupu dle rolí) (Gála, Pour a Šedivá, 2015). Klíčovou aplikací DMS je v prostředí podniku dle autorů spisová služba, která zajišťuje kompletaci a evidenci veškerých dokumentů do podniku došlých a z podniku odchozích. Archivace digitálních či digitalizovaných dokumentů by měla být řešena koncepčně a dokumenty by se měly ukládat ideálně ve formátu PDF/A , aby byly i v budoucnu stále čitelné. Dbát by se mělo i na jejich pravidelné zálohování, či obecně na archivaci dat. K tomu je nutné vybrat médium a místo záloh, naplánovat rozvrh záloh, zvolit typ zálohování – tj. například úplně nebo přírůstkové (Koch, 2010).

Systémy ECM jsou tedy více než jen prostředky pro ukládání a správu dokumentů organizace. Lakshmi (2017) uvádí, že zahrnují také nástroje, strategie a procesy používané k zachycení, uložení a správě obsahu – jedná se o velké objemy strukturovaných a nestrukturovaných dat vč. různých alternativních typů médií. DMS je tak ve svém jádru zjednodušený systém ECM, povětšinou v podobě pouze jedné aplikace. Systémy správy dokumentů jsou tak technicky podkategorií ECM, jelikož systémy ECM by nemohly existovat bez své schopnosti spravovat dokumenty.

2.9.3 Human Resources Information System

Systémy zaměřené na řízení lidských zdrojů (*Human Resource Management*, HRM) jsou dle Sodomky a Klčové (2010) nedílnou součástí podpůrných procesů prakticky veškerých podniků. Rozsah zpracovávaných informací, resp. pokrytí tohoto procesu informačním systémem je odvislé od velikosti podniku, odvětví i schopnosti efektivně IS/IT využívat. Procesy HRM jsou zakomponované v aplikacích, z nichž se skládá personální informační systém (*Human Resources Information System*, HRIS). Agenda zpracovávána HRIS zahrnuje mzdy, docházku, benefity, organizační strukturu, výběrová řízení atp.

2.9.4 Business Intelligence

Business Intelligence (BI) aplikace představují typ aplikací podporujících „*analytické, plánovací a rozhodovací činnosti podniků a organizací a jsou postaveny na principech, které právě těmto činnostem nejvíce odpovídají.*“ Jedná se o „*sadu procesů, know-how, aplikací a technologií, jejichž cílem je účinně a účelně podporovat řídící aktivity ve firmě*“. (Gála, Pour a Šedivá, 2015) Tyto aplikace nabízejí agregované i detailní informace za různě dlouhé časové období formou přehledových tabulek či grafů, které zachycují trendy či korelace (Basl a Blažíček, 2012). Aplikace BI mají dle Šilerové (2017) za cíl podporu rozhodování na všech stupních řízení a trend jejich nárůstu souvisí spolu s požadavkem na zpracování dat v reálném čase. Systémy pro manažerské rozhodování, resp. nástroje BI, získávají v posední době na oblibě zejména vlivem několika důvodů. Manažer získává jen ty informace, které jsou pro něho skutečně důležité – ty informace, které potřebuje pro své rozhodování. Úroveň detailu je variabilní a umožňuje pracovat i s velkým množstvím agregovaných dat, které je však možné hierarchicky rozložit. Systémy BI tedy mohou poskytovat výstupy (odezvu) v různých úrovních agregace dat, a to pomocí následujících funkcí (Sodomka a Klčová, 2010):

- slice-and-dice – zobrazování průřezů na základě variabilních kritérií,
- dril-down (rozpad) – zobrazení detailnějších dat pro nižší úroveň hierarchie,
- dril-up (sloučení) – zobrazení obecnějších dat pro vyšší úroveň hierarchie,
- crosstabbing (pivoting) – změna úhlu pohledu na data na úrovni prezentace DW.

Šilerová (2017) uvádí, že tyto systémy také mohou zavčas signalizovat negativní jevy či vytvářet nad daty analýzy, simulace a predikce budoucího vývoje. Výsadou aplikací BI je možnost rychle reagovat na uživatelské požadavky, pružně měnit kritéria pro analýzy, umožnit uživatelům tvořit jejich vlastní dotazy a částečně řešit problém redundance a nekonzistentnosti dat. BI aplikace jsou postaveny na principech multidimenzionálních pohledů na podniková data. Mezi BI aplikace můžeme řadit aplikace utvářející Manažerské informační systémy (MIS), které jsou schopné dodávat relevantní reporty (tj. použitelné výstupy) pro rozhodování na operativní i taktické úrovni, stejně jako Systémy na podporu rozhodování, které využívají manažeři k taktickým i strategickým analýzám (Gála, Pour a Šedivá, 2009). *„Manažerský informační systém představuje*

IS/ICT podporu pro vrcholové i operativní rozhodování, která může mít buď podobu sjednocených, předmětově orientovaných databází navržených za tímto účelem nebo jednoduchých analýz prováděných v databázích transakčních systémů" (Sodomka a Klčová, 2010).

Manažerské informační systémy pokrývají dle Šilerové (2017) všechny oblasti řízení organizace a mají na starost především evidenci a analytiku. MIS sdružují jak detailní pohledy na data, tak i různou míru abstrakce a agregace. Typický takovýto systém se skládá ze tří komponent – extrakčních nástrojů (ETL; zajišťujících přenos, čištění a konverzi dat ze zdrojových systémů do datového skladu), analytických nástrojů (užívajících statistických metod) a prezenčních nástrojů (grafické znázornění tabulek, grafů apod.).Tyto analytické systémy tedy povětšinou nevytvářejí žádná nová data, ale využívají agregace stávajících, již existujících, zdrojových dat v podniku. Na základě těchto shromážděných dat mohou zajistit vyhodnocení sledovaných metrik včetně jejich vývoje (časové řady, indexy) a analyzovat tato agregovaná data z různých dalších hledisek na rozličných úrovních detailu (*granularity*). (Gála, Pour a Šedivá, 2015) Jak uvádějí Sodomka a Klčová (2010), přínosy manažerských informačních systémů jde shrnout do tří hlavních oblastí:

- ekonomické přínosy – podpora manažerského rozhodování (omezená měřitelnost),
- přínosy plynoucí z rozvoje IT infrastruktury – např. využití DW pro integraci,
- subjektivní přínosy – zlepšení podpory rozhodování.

Výstupem aplikací BI je často vizualizace dat s využitím přehledových dashboardů obsahujících grafické vyjádření hodnot prostřednictvím grafů, tabulek či reportů. Kvalita těchto informací je do značné míry závislá na kvalitě vstupních dat z jiných aplikací. Tyto vyšší nároky na kvalitu dat plynou zejm. z výše zmíněných principů agregace, časové dimenze a multidimenzionality BI, kterou je možné vyjádřit v relačních databázích či vyjádřit prostřednictvím OLAP (On-Line Analytical Processing) technologie (Gála, Pour a Šedivá, 2015). Například Sodomka a Klčová (2010) rozlišují ještě několik variant OLAP – MOLAP (multidimenzionální OLAP), ROLAP (multidimenzionalita řešena uložením v relační databázi), HOLAP (detailní

data v relační databázi a agregace v OLAP). Gála, Pour a Šedivá (2015) dále uvádějí také například WOLAP (webový OLAP) ad.

Aplikace spadající do Business Intelligence můžeme dle autorů dále kategorizovat na aplikace na řízení podnikové výkonnosti (*Corporate Performance Management*, CPM), financí (*accounting intelligence*), marketingu (*customer intelligence* či *sales intelligence*), lidských zdrojů (např. analýza nákladů pracovní síly) ad. Současným trendem se silná tendence k samoobslužnému využití Business Intelligence – tzv. self service BI, umožňující realizaci (povětšinou individuálních či izolovaných) analytických úloh bez nutnosti používání složitých komplexních systémů či nutnosti zjišťovat informace přes více úrovní řízení, a tím zvýšit dostupnost pro uživatele vč. zkrácení potřebné doby implementace takového systému. Tyto analytické aplikace jsou relativně jednoduše ovladatelné a lze je vytvářet, resp. provozovat buď prostřednictvím specializovaných produktů nebo známých kancelářských prostředků typu MS Excel a jeho kontingenčních tabulek.

BI aplikace tedy slouží například k dotazování (query), analýzám nebo reportingu, což představuje tvorbu výstupních sestav z firemních dat, nejčastější uložených v transakčních (zdrojových, primárních) systémech, které však nejsou primárně navrženy pro analytické úlohy. BI tedy podporují řízení v reálném čase a integrují věcně či lokálně samostatné informační zdroje (Basl a Blažíček, 2012). Při stále narůstajícím objemu dat je nezbytně nutné data správným způsobem konsolidovat a vytvořit relevantní databázi výstupů, se kterou mohou koncoví uživatelé systému efektivně pracovat. Potenciálně problematická je pak zejména vhodnost výstupu (u předem nadefinovaných výstupů dochází pouze k aktualizaci dat) a aktuálnost vlastních dat. Ideálním stavem by pochopitelně bylo, pokud by si mohl každý řídící pracovník vygenerovat vlastní sestavu s aktuálními a zejména relevantními daty dle vlastního výběru, načež by mohl učinit kvalifikované rozhodnutí. V praxi však tyto nástroje nejsou vždy k dispozici pro všechny úrovně řízení. (Šilerová, 2017)

2.9.5 Portály

Portál je specifická aplikace IT tvořící univerzální rozhraní „*jehož prostřednictvím je každému (...) umožněno účastnit se procesů organizace, přistupovat ke všem relevantním informacím, komunikovat s ostatními kooperujícími pracovníky a realizovat*

adekvátní aktivity spojené s podnikovými procesy" (Gála, Pour a Šedivá, 2015). Prostřednictvím portálů jsou tedy na jednom jediném místě soustředěny informace dostupné z různých informačních zdrojů (Basl a Blažíček, 2012). Orientace a využití portálového řešení se liší napříč podniky a jejich specifickými potřebami. Gála, Pour a Šedivá (2015) dělí portály dle dominantního vztahu na ty, které podporují vztah:

- podniku a zaměstnance (business-to-employee, B2E),
- mezi podnikem a zákazníkem (business-to-customer, B2C),
- vztah mezi podniky (business-to-business, B2B).

Portály podporující vztah podniku a zaměstnance se dle autorů snaží mj. zefektivnit práci zaměstnanců podporou jejich spolupráce a zvýšením jejich komunikace, stejně jako přenesením části agendy na zaměstnance. Portály podporující vztah se zákazníky mají za cíl zvyšovat zainteresovanost klientů na podnikových procesech a aktivitách. Portály orientované na podporu vztahu s ostatními podniky se zaměřují na vytvoření integrační platformy mezi kooperujícími partnery. Portály lze samozřejmě členit i dle typu softwarového řešení na hotová komplexní řešení, řešení s vazbou na aplikační balík a technologické nástroje pro vybudování a provoz portálů. Přístup k dílčím integrovaným aplikacím a datům z prostředí portálu je realizován prostřednictvím tzv. portletů, což jsou programové komponenty generující určitý fragment funkcionality. Portály jsou často vytvářeny tak, aby byly customizovatelné a personalizovatelné, tj. přizpůsobitelné uživateli tak, aby mu byl dodáván jen relevantní obsah. Interní portál společnosti může být realizován jak formou intranetu, tak extranetu.

Do portálového řešení se integruje řada subsystémů, které jsou dostupné na jednom místě, na jediné platformě. Portál může mít například typicky formu webové aplikace. Firmy si od tohoto řešení slibují zdokonalení procesů, méně administrace, snazší přístup k relevantním informacím, sdílení znalostí a v neposlední řadě snížení nákladů (Šilerová, 2017). Dále autorka uvádí, že v podnikové praxi se podnikové portály obvykle rozdělují na:

- aplikační podnikový portál – typicky vytvářející bránu ke standardním aplikacím (transformace prezentační vrstvy),
    - informační podnikový portál
    - portál pro podporu rozhodování

- portál pro podporu spolupráce (komunikace, kolaborace)
- znalostní portál
- learning portál (vzdělávání a školení)

- virtuální portál.

2.10 Informační bezpečnost

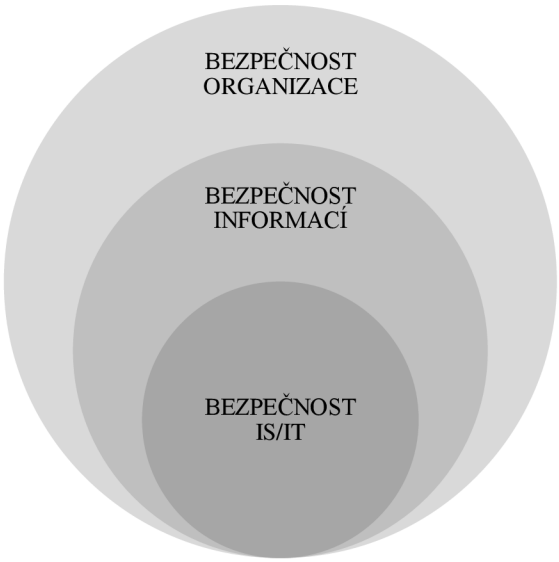
Informační bezpečnost je dle Gály, Poura a Šedivé (2009) ochrana informací před hrozbami a zranitelnostmi s cílem zabezpečit kontinuální chod činností (procesů) podniku, minimalizovat podnikatelské riziko a maximalizovat využití příležitostí. Abychom mohli identifikovat zranitelná místa, musíme nejprve identifikovat informační aktiva podniku. Aktivum je vše, co má pro jednotlivce či organizaci nějakou hodnotu. Ta je přitom závislá jak na objektivním určením ceny, tak na subjektivním hodnocení důležitosti aktiva. *„Informační bezpečnost představuje vytvoření bezpečného informačního systému (IS), v kterém je zajištěna ochrana údajů, které IS zpracovává a uchovává, tak, aby nedocházelo k úniku informací neoprávněným osobám. (...) Informační bezpečnost je proces ochrany dat před jejich náhodným anebo úmyslným zneužitím osobami v rámci anebo mimo organizaci, včetně zaměstnanců anebo hackerů.“* (Hennyeyová, 2017)

Spektrum hrozeb, resp. rizik v bezpečnosti informací, resp. oblasti IT je enormně široké. Rizika jsou navíc velmi obtížně kvantifikovatelná, což přispívá k neefektivnosti současných bezpečnostních strategií. IT bezpečnostní incidenty jsou obvykle důsledkem souběhu několika souvisejících problémů, přičemž jejich podíl na výsledku se může lišit a může být tudíž obtížné posoudit jejich relativní závažnost. Spolehlivé statistiky incidentech v oblasti IT navíc buď neexistují, nebo nejsou pro posouzení rizika příliš užitečné a případné kontrolované experimenty je v této oblasti obtížné realizovat. Výsledkem je absence užitečných modelů týkajících se rizik v IT. Problém je navíc umocněn skutečností, že IS/IT mají antagonické cíle – zajistit bezpečnost dat a usnadnit komunikaci, což musí nutně vést k určitému kompromisu. (Young, 2016)

Pojem informační bezpečnost úzce souvisí s pojmy jako je bezpečnost organizace a bezpečnost informačních systémů a informačních technologií (IS/IT), nejedná se však o synonyma. Dá se hovořit o tom, že bezpečnost organizace je informační bezpečnosti

nadřazená, a naopak bezpečnost IS/IT je podskupinou bezpečnosti informací. Nicméně například Gála, Pour a Šedivá (2009) informační bezpečnost vyčleňují, jelikož (opačným směrem) definují, že bezpečnost IS/ICT zasahuje do následujících oblastí:

- oblast objektové bezpečnosti (budov a prostor),
- oblast bezpečnosti a ochrany zdraví (vč. ergonomie),
- oblast informační bezpečnosti (bezpečnost informací ve všech jejich formách a během jejich celého životního cyklu; orientována na zachování důvěrnosti, integrity a dostupnosti a s nimi spojené priority jako je autentičnost, odpovědnost, nepopiratelnost a hodnověrnost).



Obrázek č. 8: Vztah úrovní bezpečnosti v organizaci
(Zdroj: vlastní zpracování dle Hennyeyové, 2017)

Komponenty IB, respektive vztah jednotlivých úrovní bezpečnosti v organizaci:

- bezpečnost organizace – bezpečnost objektů a majetku organizace,
- bezpečnost informací – zásady práce s informacemi – zahrnuje také způsob zpracování a archivace dat vč. uložení a správy archivů nedigitálních dat, zásady likvidace dat (skartace, ad.),
- bezpečnost IS/IT – bezpečnost informačních systémů a informační (a komunikační) techniky.

Pro oblast řízení informační bezpečnosti ve vztahu k IT existuje řada uznávaných mezinárodních doporučení, či přímo standardů ISO (resp. ISO/IEC), o které se lze při tvorbě a řízení IB opřít. Mezi nejznámější patří ITIL, COBIT (základní principy znázorněny tzv. COBIT kostkou) a ISO/IEC 27000, nicméně existuje i celá řada dalších, méně známých či méně komplexních standardů a metodik. Obecně jde však říci, že se vždy opíráme buď o „de iure" standardy (např. ISO řady 27000) nebo „de facto" standardy (např. ITIL), které vždy formulují jak proces, tak obsah řešení problematiky informační bezpečnosti v organizacích. Dle definice mezinárodního standardu ISO/IES 27 001 zahrnuje informační bezpečnost 3 hlavní principy (Hennyeyová, 2017), resp. bezpečnostní požadavky (Gála, Pour a Šedivá, 2009):

- důvěrnost (*Confidentality*),
- integrita (*Integrity*),
- dostupnost (*Availiability*).

Princip důvěrnosti spočívá v tom, že informace nejsou zpřístupňované a odhalované neautorizovaným osobám, entitám nebo procesům. Jedná se o atribut údaje (dat), který definuje, že tato informace nebude poskytnuta, odhalena nebo zneužita neoprávněným subjektem. Představuje tak hierarchicky uspořádaný mechanismus, který zaručí požadovaný stupeň oprávnění na zápis a čtení údajů v určené části zabezpečovacího systému. Porušení principu důvěrnosti může způsobit, že tyto údaje budou dostupné neautorizovaným jednotlivcům nebo procesům.

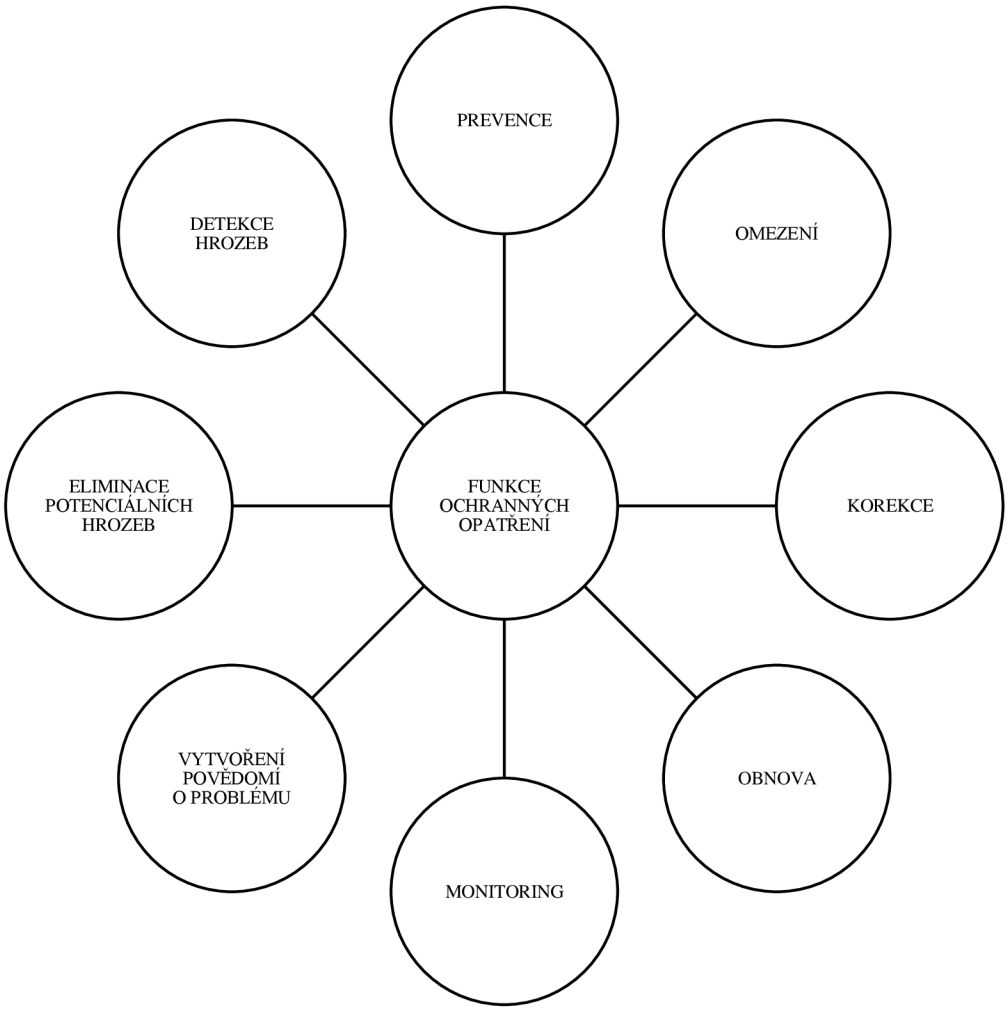
Princip integrity znamená zabezpečení přesnosti a úplnosti aktiv. Tento princip reprezentuje neporušitelnost vložených údajů zásahem ať už v technické části systému (např. selhání hardware) nebo lidského faktoru. Obecně se rozlišuje integrita údajů (před změnou dat nebo zničením neautorizovaným zásahem) a integrita systému (ochrana IS jako celku). Narušení této integrity znamená neautorizované stažení (příjem dat), nahrání (vysílání dat) nebo změnu údajů. Princip dostupnosti je schopnost aktiv být dostupná a použitelná na požádání autorizované entity (subjektu). Existuje časová charakteristika vyjadřující závislost mezi požadavky řízeného systému a splněním těchto požadavků. Vyjadřuje se pravděpodobností zpoždění mezi žádostí o službu a její realizací. Ztráta dostupnosti může znamenat nepřístupnost, a tedy nepoužitelnost informačního systému (autorizovaným jednotlivcem nebo procesem) v požadovaném

čase. Tyto tři principy jsou známe též pod zkratkou CIA (*Confidentality, Integrity, Availiability*). Tato norma (ISO/IES 27001), tedy systém řízení bezpečnosti informací, je částí celkového systému řízení organizace, resp. přístupu organizace (podniku) k rizikům činnosti, která je zaměřená na ustanovení, zavádění, provoz, monitorování, přezkoumání, udržování a zlepšování bezpečnosti informací. Tento přístup bezpečnostního projektu zavádění ISMS vychází z tzv. Demingova modelu či cyklu (PDCA). Co se dalších atributů týče, v praxi je obvykle důležité zajistit také autentizaci (tj. ověření, že je subjekt skutečně tím, za koho se vydává), autorizaci (tzn. omezení dostupnosti určitých operací v závislosti na oprávnění) a nepopiratelnost (tj. vyloučení možnosti popření určité provedené operace). Podle způsobu možného útoku na tyto atributy v praxi můžeme rozlišovat následující oblasti informační bezpečnosti (Gála, Pour a Šedivá, 2009):

- fyzická bezpečnost,
- komunikační bezpečnost,
- počítačová bezpečnost,
- logická bezpečnost,
- personální bezpečnost.

Fyzická bezpečnost dle autorů zahrnuje působení hrozeb na samotná aktiva, která jsou součástí IS. Jedná se tedy o ochranu proti neoprávněnému zásahu osob, způsob likvidace nepotřebných informací, ochranu proti požáru, záplavám, přírodním živlům, stejně jako řešení krizových situací atd. Komunikační bezpečnost je působení hrozeb na nehmotná aktiva během jejich zpracovávání, distribuce a ukládání. Spadá sem například ochrana dat v databázích proti modifikování, odcizení či ztrátě, ale také zachování důvěrnosti přenášených zpráv. Počítačová bezpečnost znamená působení hrozeb na hmotná aktiva IS, tj. hardware. Zahrnuje celou šíři problematiky HW – od výběru spolehlivých prostředků, až po servis a údržbu. Logická bezpečnost zahrnuje působení hrozeb na nehmotná aktiva IS, která jsou nezbytná pro fungování systému z hlediska řízení přístupu k informacím. Jde tedy zejména o nastavení software vč. operačních systémů tak, aby byla zabezpečena kontrola přístupu, autorizace a autentizace uživatelů, rozdělení a přidělení přístupových práv a pravomocí a sledování a zaznamenávání

činností (logy). Personální bezpečnost se zaobírá eliminací hrozeb způsobených lidským faktorem, tedy primárně uživateli IS. Definuje personální pravomoci a zodpovědnosti jednotlivých pracovníků, kteří mají do systému přístup. Ochrany informací kolujících v podniku můžeme dosáhnout implementací různých protiopatření jako jsou nejrůznější bezpečnostní politik, nastavené procesy a postupy, speciální organizační struktury či softwarová a hardwarová opatření. Tato opatření je nutné nejprve implementovat a posléze monitorovat, analyzovat a zlepšovat všude tam, kde je to potřebné pro splnění specifických bezpečnostních záměrů podniku.



Obrázek č. 9: Funkce ochranných opatření
(Zdroj: vlastní zpracování dle Hennyeyové, 2017)

Někteří autoři, např. Hennyeyová (2017), člení ochranná opatření dle oblastí na:

- opatření v oblasti fyzické bezpečnosti – např. přístup, záložní zdroje, dostupnost komponent,
- opatření v oblasti informační bezpečnosti (technologická) – HW a SW,
- režimové a organizační opatření (administrativní) – pravidla, vzdělávání uživatelů apod.

Opatření jde však členit dle autorky i dle časového hlediska a to na:

- preventivní – účelem je minimalizovat příčiny možného vzniku bezp. incidentu,
- dynamická (proaktivní) – možné dopady aktuálně probíhajícího bezp. incidentu vč. včasného zachycení,
- následná (reaktivní) – minimalizovat možné dopady proběhnuvšího bezpečnostního incidentu.

Dopady rizik v oblasti bezpečnosti informací mohou být dle Hennyeyové (2017) nejen v oblasti finanční nebo obchodní, ale také právní a regulatorní. Různé stupně zabezpečení vyžadují různé kombinace opatření. Tato problematika úzce souvisí s řízením rizik, jelikož se používají postupy obecně známé z risk managementu. Identifikované riziko můžeme akceptovat, snížit, maximálně eliminovat nebo přesunout (transferovat), přičemž musíme dávat pozor na provázanost celého systému informační bezpečnosti ve všech jejích oblastech. Nerozpoznané slabé místo může potenciálně vést k narušení či dokonce zhroucení celého IS. Obecně by mělo by platit, že náklady na ochranná opatření by neměly být vyšší než očekáváné ztráty v důsledku výskytu bezpečnostního incidentu. Informační bezpečnost však nespočívá pouze v zavedení technických opatření. V organizacích je vhodné budovat a upevňovat „kulturu bezpečnosti“, jakožto prostředku povědomí a porozumění otázkám informační bezpečnosti, který podněcuje všechny účastníky (tj. zejména pracovníky a uživatele) k vyšší míře naplňování principů informační bezpečnosti. Jedná se o způsob myšlení, hodnocení a konání při provozování informačních systémů a sítí, povědomí o rizicích ohrožujících informační systémy a zásadách, praktikách a protiopatřeních, stejně jako o potřebě jejich přijetí a implementace. (Hennyeyová, 2017)

2.10.1 Bezpečnostní politika

Bezpečnostní politika informací podniku, která prostupuje celou jeho strukturou a je navázána na další procesy, by měla dle Gály, Poura a Šedivé (2009) vycházet z celkové koncepce bezpečnostní politiky organizace a navazovat na souhrn ochranných opatření vypracovaných v rámci ochrany majetku, BOZP apod. Bezpečnostní politika by měla mít formu písemného dokumentu, ve kterém budou shrnuty komplexní představy vedení o řešení bezpečnosti a měla by obsahovat také vymezení základních požadavků na jednotlivé bezpečností oblasti celého informačního systému a jeho součástí, bezpečnosti přenosu, zpracování a uchovávání informací a především, vymezení personální zodpovědnosti za jednotlivé dílčí oblasti. Budování bezpečností politiky organizace, a zvláště pak vzdělávání zaměstnanců, je vysoce důležité, protože se obecně udává, že převážná většina hrozeb (více než 50 %) patří do kategorie neúmyslných. „*Bezpečnostní politika je v praxi vnímána jako základní východisko pro řízení bezpečnosti IS*“ (Hennyeyová, 2017).

Bezpečnostní politika je dle Gály, Poura a Šedivé (2009) „ *soubor zásad a pravidel, s jejichž pomocí organizace chrání svá aktiva“*. Bezpečnostní politika je kontinuálně aktualizována v souladu se změnami prostředí a může zahrnovat:

- politiku přípustného užívání aktiv,
- specifikaci vzdělávacího procesu svých zaměstnanců v oblasti ochrany aktiv,
- objasnění způsobu uskutečňování a vynucování bezpečnostních opatření,
- proceduru vyhodnocení účinnosti politiky vedoucí k provedení její změny.

Bezpečnostní politika organizace tedy deklaruje bezpečnostní cíle a definuje zásady procesu ochrany informací, pravidla, postupy a omezení, které určují způsob správy, ochrany a distribuce citlivých informací obsažených v informačním systému. Cílem této podnikové politiky je identifikovat relevantní hrozby a minimalizovat vliv rizik, a to právě prostřednictvím zmíněných pravidel a postupů pro konkrétní informační systém. Výsledný souhrn ochranných opatření zahrnuje řešení informační bezpečnosti v oblasti fyzické, komunikační, IT, logické i personální. Mezi základní otázky patří *„Co chceme chránit? Proč? Jak? Co budeme dělat, když dojde k selhání?“* (Hennyeyová, 2017) V souvislosti s kulturou bezpečnosti je v podniku také vhodné budovat a podporovat

tzv. *Security Awareness Education* (SAE) jakožto součást firemní kultury – tedy zvyšovat povědomí zaměstnanců (uživatelů) o informační bezpečnosti a zvyšovat jejich informační gramotnost.vPodle stupně zabezpečení je možno definovat čtyři obecné typy bezpečnostní politiky (Gála, Pour a Šedivá, 2009):

- promiskuitní – nic neomezuje, povoluje subjektům vše včetně toho, co by neměly konat,
- liberální – umožňuje realizovat vše až na explicitně vyjmenované výjimky,
- opatrná – ve svých pravidlech a předpisech zakazuje takřka vše až na explicitně vyjmenované výjimky,
- paranoidní – zakazuje dělat vše potenciálně nebezpečně vč. toho, co by nemuselo být explicitně zakázáno.

Při nastavování bezpečnostní politiky podniku musíme kromě ekonomického porovnání nákladů na opatření vs. hodnoty informací brát v úvahu i stávající procesy ve firmě, jelikož striktní bezpečnostní politika může vést k přílišnému omezování zaměstnanců a v důsledku tak ke snižování efektivity práce. *„Dobře navrhnutá bezpečností politika je kompromisem mezi omezováním uživatelů a chráněným zájmem organizace.“* (Hennyeyová, 2017)

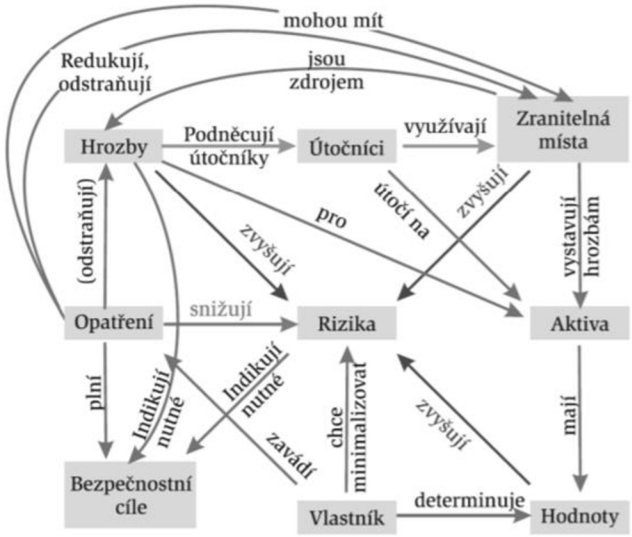
Mezi obecná doporučení na zlepšení, resp. zvýšení úrovně informační bezpečnosti podniku, dle autorky pak patří:

1) definování přístupových práv uživatelů IT/IS (jen minimální nutná),
2) definování zodpovědnosti uživatelů IT/IS za vznik a řešení bezpečnostních incidentů (pravidla použití, povinnosti),
3) klasifikace informací v podniku podle citlivosti (např. veřejné, interní, chráněné)
4) odhalení a řešení bezpečnostních incidentů (vypracování zásad, řešení, přijetí opatření),
5) definování aktiv v podniku (vše, co má hodnotu je nutné chránit),

6) vzdělávání v oblasti bezpečného využívání IT/IS v podniku, které je systematické, nepřetržité).

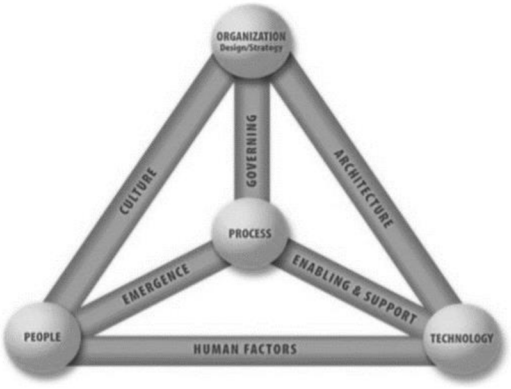
2.10.2 Vybrané modely informační bezpečnosti

Ohledně informační bezpečnosti vznikla celá řada konceptů a teoretických modelů, některé jako součástí ucelených metodik (např. COBIT), jiné jsou samostatné a mají za cíl znázornit vztahy v oblasti informační bezpečnosti, popř. ICT.



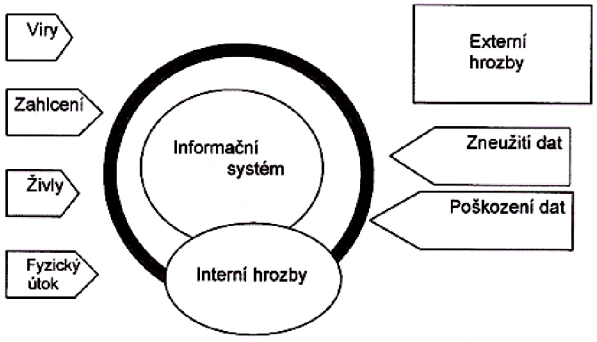
Obrázek č. 10: Obecný model bezpečnosti informačních technologií
(Zdroj: Hanáček a Staudek, 2000)

Obecný model informační bezpečnosti například znázorňuje vztahy mezi vlastníkem, riziky, hrozbami, útočníky, zranitelnými místy, aktivy, hodnotami, bezpečnostními cíli a opatřeními.



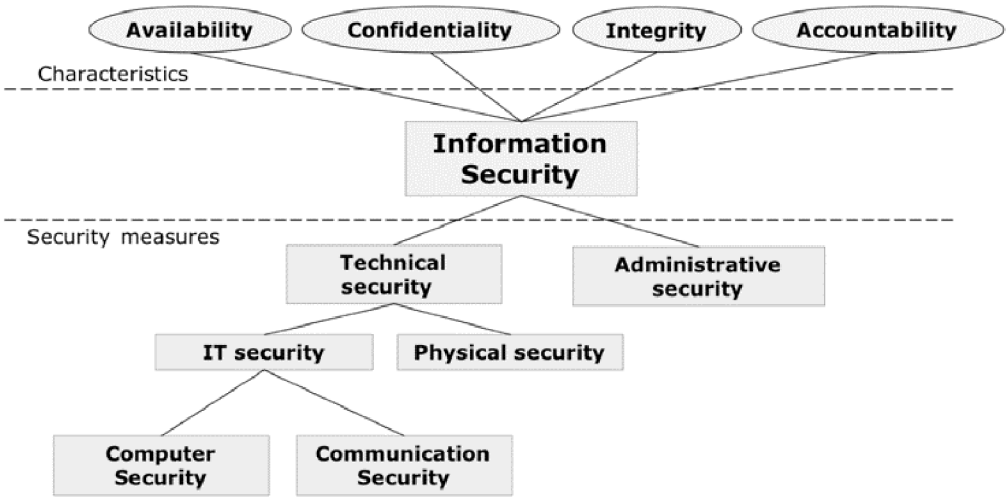
Obrázek č. 11: Business Model for Information Security
(Zdroj: ISACA)

Business model pro bezpečnost informací (BMIS) vytvořila asociace ISACA zaměřující se na problematiku auditingu bezpečnosti informačních systémů. Tento model tvoří Organizace, Procesy, Lidé a Technologie, přičemž tyto Výše uvedené prvky BMIS modelu jsou dohromady propojeny pomocí dynamických propojení a vytváří tak všestrannou sílu (Správa, Kultura, Rozvoj, Umožnění a podpora, Architektura, Lidské faktory).



Obrázek č. 12: Informační systémy a jejich bezpečnost
(Zdroj: Koch, 2010)

Koch (2010) ve své infografice znázorňuje interní hrozby, externí hrozby a rizika působící na informační systém. Těmito riziky je zneužití či poškození dat prostřednictvím virů, zahlcení, živlů nebo fyzického útoku.



Obrázek č. 13: Rozšířený InfoSec model
(Zdroj: Áhlfeldt, Spagnoletti a Sindre, 2007)

Information Security model se ubírá cestou vlastností, resp. principů, které působí na informační bezpečnost, kterou lze rozdělit do několika oblastí. V InfoSec jsou vyznačeny základní oblasti IB:

- administrativní – admin. a organizační pravidla (definování bezp. politiky, vzdělávání uživatelů, …),
- fyzická – fyzické zajištění aktiv (přístup, ostraha, záložní zdroje, dostupnost náhradních komponent, …),
- technologická – HW a SW (zálohování, šifrování, politika hesel, automatický monitoring sítě, automatická blokace či odstavení).

2.11 Trendy

Informační a komunikační technologie jsou prudce se rozvíjejícím odvětvím. Cílem této části je popis dlouhodobých trendů v oblasti ICT významně ovlivňujících soudobé informační systémy, jež se vztahují tématu této práce.

2.11.1 Cloud Computing

Cloud Computing (CC) je model dodávky ICT produktů, resp. model poskytování IT služeb (Basl a Blažíček, 2012). Tento model poskytování IT služeb lze obecněji nazvat *Aplication Service Providing* (ASP) (Koch, 2010). Základní principy CC lze spatřit již v poskytování e – mailových služeb nebo hostingu, avšak od těchto služeb se CC odlišuje zejména tím, že z pohledu zákazníka je primární motivací redukce nákladů na provoz ICT (Basl, 2011). Tento model je dnes hojně užíván zejména díky rozvoji internetu, skrze který jsou služby přístupné, a informačních technologií. Cloud Computing je model umožňující všudypřítomný, rychlý, pohodlný a na žádost realizovaný přístup, kladoucí minimální požadavky na uživatele (i komunikaci s poskytovatelem), ke sdílitelným a konfigurovatelným výpočetním prostředkům (síť, výkon, úložiště atp.) (Mell a Grance, 2011). Podstatným rysem Cloud Computingu je, že koncový uživatel povětšinou neví a obvykle ani nepotřebuje vědět, kde jsou fyzicky uložena data jím používaných aplikací (Basl, 2011).

Cloud Computing se dle Gály, Poura a Šedivé (2015) vyznačuje následujícími schopnostmi:

- dodat požadované kapacity kompletního systému zpracování dat uživateli neviditelně (virtualizace),
- dynamicky propojit IT a techniku a tím uživatelům poskytovat spolehlivý, všudypřítomný a levný přístup ke špičkovým výpočetním službám (grid),
- překonat různorodost prostředků, které existují v PIS (Service-oriented Computing),
- zajistit přípravu prostředí a následné účtování uživatelem spotřebované služby.

S modelem Cloud Computingu je spjato pět charakteristik, tři základní modely služeb a čtyři modely nasazení (Mell a Grance, 2011):

- systém je samoobslužný – zákazník/uživatel může měnit úroveň poskytovaných služeb bez nutnosti zásahu technika,
- existuje všestranný síťový přístup – služby jsou dostupné prostřednictvím internetu s použitím různých klientů či zařízení,
- existuje zde sdílení zdrojů – dynamické sdílení zdrojů cloudu mezi několik uživatelů – tzv. multi-tenancy model, zákazník si povětšinou konfiguruje maximálně umístnění datacentra, charakteristiky je možné upravit smlouvou upravující rozsah a provozní specifikace, jako např. dostupnost, dobu odezvy atp. – *Service Level Agreement* (SLA) (Molnár, 2001). Kromě SLA existují také doplňující dohody zvané *Operational Level Agreement* (OLA) (Koch, 2010),
- existuje zde okamžitá škálovatelnost a elasticita – zákazník si může určit maximální výkon cloudu (tarif), popř. využívá automatické škálování dle potřeby,
- konzumace služeb je měřena – systém optimalizuje využívané zdroje a účtuje zákazníkům (pay-as-you-go, tarify, balíčky apod.).

Rozlišujeme tři základní modely služeb Cloud Computingu, z nichž zřejmě nejznámější je poskytování software jako služby (*Software as a Service*, SaaS). Dle Basla a Blažíčka (2012) jsou tímto způsobem zákazníkovi poskytovány aplikace na platformě či infrastruktuře poskytovatele, a to na bázi předplatného. Uživatel si tedy nic nekupuje, ale vše si pronajímá od třetí strany. Dalším distribučním modelem služeb Cloud

Computingu je poskytování výpočetní platformy jako služby (P*latform as a Service*, PaaS), kdy jsou zákazníkovi poskytovány kompletní prostředky, které mu umožní vyvinout aplikaci a poté ji provozovat, popř. je mu umožněno provozovat aplikaci získanou od třetí strany. Posledním základním modelem je poskytování infrastruktury jako služby (*Infrastrucutre as a Service*, IaaS). V takovém případě jsou zákazníkovi poskytovány přímo výpočetní zdroje, na které si může nasadit libovolný software (Mell a Grance, 2011). Jedná se například o pronájem virtuálního serveru (Virtual Private Server, VPS). SZ hlediska způsobu nasazení se rozlišují čtyři základní modely cloudových služeb (Mell a Grance, 2011):

- veřejný cloud,
- privátní cloud (poskytnutí vlastního Cloud Computingu sobě či svým organizačním jednotkám),
- komunitní cloud (společný),
- hybridní cloud (více propojených cloudů zajišťující přenositelnost obsahu a efektivní nakládání s prostředky).

2.11.2 BYOD

Pojmem BYOD neboli *Bring-Your-Own-Device*, se označuje politika, v níž je zaměstnancům firmy (popř. dalším uživatelům) umožněno využívat vlastních (přenosných) zařízení při přístupu k podnikovým datům a aplikacím (Gála, Pour a Šedivá, 2015). Politika BYOD je v podnicích na vzestupu i díky stále pokračujícímu trendu zvyšující se dostupnosti výkonných mobilních zařízení na straně jedné a s postupnou akceptací tohoto trendu v podnikovém prostředí na straně druhé. Tento přístup je však kromě řady výhod, jako je například úspora nákladů a příjemnější používání pro zaměstnance, také spojen s celou řadou rizik vztahujících se zejména k bezpečnosti podnikových dat, resp. informační bezpečnosti. Nejedná se přitom pouze o riziko ztráty či kompromitace dat, ale také o způsob likvidace vyřazených zařízení či dodržování pravidel komunikace. Mezi největší zranitelnosti se v souvislosti s BYOD hovoří zejména o nekonzistentnosti zásad zabezpečení, úniku informací na sdílených médiích, minimální správě zařízení nebo úniku dat mezi aplikacemi (Girard, 2013).

Analogicky s BYOD se objevuje i termín BYOC (*Bring-Your-Own-Cloud*), což je trend či koncept využívání cloudů třetích stran zaměstnanci podniku, čímž se mj. zvyšuje

riziko ztráty dat vlivem chybějící kontroly nad nimi, stejně jako riziko chyby či omezená kompatibilita vlivem využívání nekonzistentních systémů (Kemp, 2014). Toto řešení však sebou nese i řadu výhod – zaměstnanci mohou vykonávat svoji činnost mnohdy více efektivně, jelikož práce v daném systému je pro ně pohodlná a intuitivní a podniková informatika zkrátka nenabízí lepší alternativu.

2.11.3 Gamifikace

Gamifikace je prostředek, který pomáhá zvyšovat zájem zákazníků (či zaměstnanců) pomocí užití herních prostředků, herních designů, herního myšlení a herních principů v neherních oblastech, jakými jsou například webové či mobilní aplikace. Tato technika je dnes v určité podobě uplatňována prakticky ve všech odvětvích v celé řadě služeb.

Cílem gamifikace je vylepšit systémy, služby, organizace a aktivity s cílem vytvořit podobné zážitky jako při hraní her a tím více motivovat a zapojit uživatele (Hamari, 2021). Termín „gamifikace“ se poprvé objevil v souvislosti s počítačovým softwarem v roce 2008 (Walz a Deterding, 2015). Dříve byla gamifikace po relativně dlouhou dobu chápána především jako začleňování sociálních a „prémiových“ aspektů her do neherního prostředí ostatního software. Co se však samotného pojmu týče, někteří kritici, např. Bogost (2011), namítají, že se prakticky nejedná o nový směr marketingu, jako spíše o k dokonalosti dotažené ocenění za věrnost.

Gamifikace využívá přirozené hravosti lidí – touhy lidí po socializaci, učení, mistrovství, soutěži, úspěchu, postavení, sebevyjádření, altruismu nebo nebo jednoduše jejich reakce na rámování (framing) dané situace jako nějaké hry (Lieberoth, 2015). Samotné nástroje gamifikace stojí na rozsáhlých znalostech lidské psychologie. Existuje mimo jiné i obecná typologie lidí, hráčů, dle motivace. Kupříkladu prof. Richard Bartle popisuje 4 následující skupiny: „*Archiever*“, „*Socialiser*“, „*Explorer*“ a „*Killer*“. Například tzv. Achievers, jsou hráči, kteří se snaží být nejlepší, snaží se ukázat ostatním a jde jim primárně o výhru a splnění předem stanovených cílů. Tato skupina lidí však nerada prohrává a pokud jim tedy není opakovaně dopřána možnost dosáhnout úspěchu, často o hru rychle ztratí zájem. (Kumar, Herger a Friis Dam, 2020) Častým gamifikačním nástrojem je také *progress bar*, který je častou grafickou vizualizací postupu. Často je možné se setkat také s různými odznáčky či avatary za splněné úkoly a s dalšími interaktivními gamifikačními prvky. Společně s gamifikací se často využívá

i tzv. tokenizace, což je použití virtuálních měn (např. bodů) namísto klasické měny, což přispívá k větší interakci uživatele. Samozřejmostí u všech těchto gamifikačních nástrojů je uživatelsky přívětivý design celého prostředí (UX i UI).

Obecně můžeme gamifikaci dělat například podle zaměření na interní a externí. Interní gamifikace cílí především na zaměstnance společnosti a vnitřní procesy ve firmě. Zavádění gamifikačních prvků do těchto procesů má za primární cíl zvýšení motivace zaměstnanců. Typicky tento způsob motivace funguje tak, že zaměstnanci získávají za své pracovní úsilí či svůj pracovní rozvoj určité body. Výstupem bodování je umístnění na určitém žebříčku a z toho plynoucí zisk určitého finančního či nefinančního ocenění. Zaměstnanci také často soutěží mezi sebou či celými odděleními. Tento systém tedy slouží ke zvýšení motivovanosti a angažovanosti zaměstnanců, inovacím firemní kultury a v neposlední řadě k posílení interní komunikace (jelikož jsou tyto systémy často nasazovány v interních IS). Externí gamifikace naopak cílí na zákazníky vně dané firmy a slouží k marketingovým (i obchodním) účelům – zejména prohloubení vztahu k dané službě a většímu angažování zákazníka do celého procesu.

K propojení designu her a designu služeb začalo docházet relativně nedávno. Na gamifikaci ve službách se začalo hledět jako na jakési vylepšení základní služby nabízené zákazníkům. *„Gamifikace je forma balíčkování služeb, kdy je základní služba rozšířena o systém služeb založený na pravidlech, který uživateli poskytuje zpětnou vazbu a mechanismy interakce s cílem usnadnit a podpořit celkovou tvorbu hodnoty pro uživatele“* (Huotari a Hamari, 2011).

Designéři služeb tak intenzivně hledají způsoby, jak zlepšit uživatelskou zkušenost a zvýšit zapojení uživatele ve službách (Klapztein a Cipolla, 2016). Při implementaci gamifikačních nástrojů však musíme přesně vědět co chceme, aby tato cílová skupina uživatelů dané služby dělala, a jakým způsobem ji tedy mají tyto nástroje pomoci změnit její chování. Určité metody gamifikace dnes využívá ve své podstatě značná část služeb, zejména pak aplikací. Jedná se i o takřka všudypřítomné health-trackery, které nás motivují ke sportu a odměňují nás, když se hýbeme. Gamifikace tedy může i rutinní procesy činit více zábavnými.

Nesmíme však také ignorovat, že příliš horlivé zapojení těchto mechanismů do lidského života může být kontraproduktivní a vést k negativním konsekvencím. Používání

gamifikačních metod je mnohdy kontroverzní, jelikož je jejich prostřednictvím možné vyvolat závislost uživatele na dané službě – jedná se například o používání těchto systémů v online hazardních hrách, kde vedou k prodloužení „životního cyklu“ hráčů a tím k prohloubení jejich ztrát. Hodně diskutovaná je také role gamifikace v tzv. systému sociálních kreditů v Číně (Jirouš, 2019).

2.11.4 User experience design (UX)

User experience design (UX) je dle Koďouskové (2022) soubor metod a zásad používaných k zajištění kvalitního uživatelského zážitku při provozování určitých produktů – např. webových stránek nebo mobilních aplikací, byť v širším slova smyslu můžeme UX vztáhnout např. i ke spotřební elektronice, nápojovým automatům nebo automobilům. User experience design tedy souvisí s designem služeb obecně (*Service design*).Cílem UX je dosáhnout funkčního a užitečného produktu především díky intuitivnímu ovládání. Tímto způsobem bude dosažena spokojenost uživatele, resp. zákazníka. Interakce byla tedy měla být vždy co nejjednodušší a snadno srozumitelná – v této souvislosti se hovoří o tzv. *User-centered designu* (UCD), popř. *Human-cenetered designu* (HCD). UX designer při svých návrzích využívá detailní analýzy požadavků jak firmy, tak především zákazníka – každý design je tak vytvořen na míru jak digitálnímu produktu, tak jeho cílové skupině. Určité požadavky kladené na interakci mezi uživatelem a uživatelským rozhraním (či obecněji mezi člověkem a strojem) jsou také standardizovány – např. v ergonomické normě ISO 9241. UX design tedy úzce souvisí s marketingem, jelikož bere v potaz např. vzhled obalu, způsob distribuce apod. v souladu s jednotným stylem firemní identity, ale souvisí zejména s psychologií (viz. gamifikace). Jedná se dynamicky vyvíjející se odvětví, ve kterém není o nejrůznější trendy nouze. UX designer by měl být schopný se empaticky vcítit do role uživatele a analyzovat cílové skupiny (s vhodným zacílením pomůže např. vytváření person). Je třeba brát v potaz, že u každé služby existuje několik skupin uživatelů, lišících se svým očekáváním, a tudíž je jim nutné přizpůsobit funkcionality i vzhled produktu. Před finálním spuštěním produktu by měla následovat fáze testování a získat zpětnou vazbu. Nepřehledné uživatelské rozhraní, nevhodné umístnění ovládacích prvků nebo například nedořešená přístupnost (např. pro zrakově postižené) může být vážnou překážkou v bezproblémovém používání produktu. Kvalitní UX design pomůže diferenciovat se od konkurence. (Koďousková, 2022)

UX design je dle autorky často zaměňován s UI designem, který je také nedílnou součástí vývoje aplikací. Design uživatelského rozhraní (*User Interface*, UI), resp. UI design je proces návrhu uživatelských rozhraní pro zařízení a software tak, aby bylo dosaženo maximální použitelnosti a co nejlepšího uživatelského zážitku. UI však představuje spíš jakýsi obal produktu – zaměřuje na to, jak daný web nebo aplikace vypadá, je tedy spíše nástrojem realizace UX designu.

2.12 Řízení změn IS/IT

Změny v oblasti IS/IT probíhají víceméně vždy formou projektů, ať se jedná o tvorbu nového informačního systému, jeho implementaci, úpravu či upgrade a do určité míry je na ně možné aplikovat tradiční přístupy projektového řízení včetně například stanovení efektivnosti jejich přínosů (Basl a Blažíček, 2012). Projekty se od provozních činností v podniku liší tím, že končí ve chvíli, kdy je dosaženo jejich cílů nebo když je projekt ukončen (Schwalbe, 2011). Specifika a odlišnosti plynou, dle Basla a Blažíčka (2012), vyjma jejich hmotné stránky (HW), zejména z jejich nehmotné stránky, která je neoddělitelnou součástí IS. V rovině sociálně psychologické se pak jedná o poněkud komplikovaný vztah pracovníků ke změnám, změna IS zpravidla vyžaduje také nutné proškolení a celkově změna představuje poměrně výrazný zásah do podnikových procesů, strategie, podnikové kultury i způsobu komunikace. *„Na rozdíl od projektů z jiných oblastí mohou být ty informační velmi různorodé. Některé se týkají pouze několika lidí instalujících nakoupený hardware a software. Jiné zahrnují stovky lidí analyzujících několik obchodních procesů organizace a následně společně vyvíjejících nový software za účelem dosažení podnikových cílů.“* (Schwalbe, 2011)

Projekty v oblasti IT však s sebou přináší určitá specifika. Sodomka a Klčová (2010) specifikují čtyři společně se vyskytující znaky s těmito specifiky:

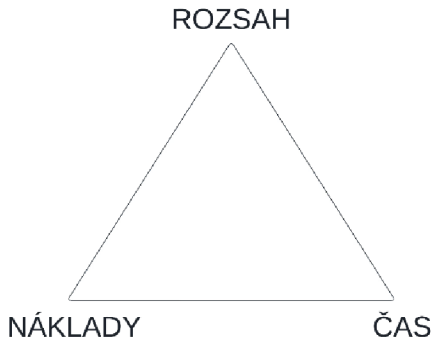
- cíl projektu je vždy trojrozměrný (viz. projektový trojimperativ),
- projekt je jedinečný (neopakovatelný či pouze do určité míry opakovatelný),
- projekt je realizován za běžného provozu organizace (sladění s cíli organizace),
- projekt je realizován vždy za využití lidských a materiálových zdrojů.

Schwalbe (2011) udává ještě další atributy každého projektu:

- dočasnost – tj. má jednoznačný začátek a konec,

- vytváření postupným rozpracováváním – přírůstkový vývoj,
- existence primárního zákazníka nebo sponzora,
- nejistota součástí projektu.

Projektový trojimperativ neboli trojí omezení (*Triple Constraint*) dle autorky graficky znázorňuje, že každý projekt je limitován svým plánovaným rozsahem, časem a náklady. Projektový trojimperativ ilustruje provázanost a jistou protichůdnost těchto omezujících faktorů, resp. základních elementů každého projektu – totiž změna jednoho z parametrů vede ke změně minimálně jednoho dalšího. Dalším z klíčových faktorů, který se někdy do těchto znázornění promítá je kvalita, která úzce souvisí se spokojeností zákazníka či sponzora – vzniká pak tzv. projektový čtyřimperativ.



Obrázek č. 14: Projektový trojimperativ
(Zdroj: autor)

Pro úspěšně dosažení cíle je tedy nutné udělat kompromis mezi výše uvedenými limitujícími faktory – tj. například abychom dosáhli plánovaného rozsahu a trvání projektu, bude nutné zvýšit jeho rozpočet. Na projektovém manažerovi zůstává rozhodnutí, který z aspektů projektového trojimperativu je pro projekt nejdůležitější (Schwalbe, 2011).

Zainteresované strany projektového řízení tvoří lidé, kteří jsou buď do projektu přímo zapojeni nebo se jich projektové aktivity nějakým způsobem dotknou. Patří mezi ně sponzor projektu a projektový tým a dále pak např. podpůrný personál, zákazníci, dodavatelé ad. (Schwalbe, 2011). Projektový manažer musí rozvíjet některé klíčové kompetence a používat některé z nástrojů a technik projektového řízení ať už v oblasti řízení rozsahu a času nebo v oblasti řízení kvality, HR, komunikace (např. komunikační plány či kick-off meetingy) či rizik (Schwalbe, 2007). Projekt je úspěšný, pokud splnil stanovený rozsah, cíle a náklady, jeho zákazník či sponzor je s ním spokojen a pokud

výsledky naplnily hlavní účel projektu (např. úspora nákladů, návratnost investice apod.) (Schwalbe, 2011).

V projektovém řízení se dle autorky uplatňuje tzv. systémový přístup. Ačkoliv je jednodušší se zaměřit na někdy zúžené zájmy daného konkrétního projektu, je bezpodmínečně nutné řídit projekty s ohledem na jejich okolní prostředí, v kontextu potřeb dané organizace. Tento holistický přístup se promítá v modelu tří oblastí systémového řízení, který zahrnuje oblast obchodní, organizační a technologickou. Na organizace pak lze nahlížet z pohledu čtyř různých rámců – strukturálního (znázorněn organigramem), politického, symbolického a rámce lidských zdrojů. Podniky mohou mít různou organizační strukturu (např. funkční, maticovou ad.), které se vzájemně liší zejména přístupem k řízení, ale i dalšími významnými aspekty. I z tohoto důvodu je vhodné přistupovat k problematice řízení projektů komplexně a systematicky – viz. integrované řízení projektu. Integrované řízení projektu zahrnuje koordinaci všech znalostních oblastí projektového řízení napříč životním cyklem projektu. K řízení projektů je možné také využít nejrůznějších softwarových prostředků.

Informační projekty, resp. ty zaměřené na IS/IT, je možné kategorizovat například z hlediska celkové priority projektu, časového okna nebo z hlediska impulsu pro projekt. Z tohoto hlediska je dělíme na (Schwalbe, 2011):

- problémy – tj. nežádoucí situace, které společnosti zabraňují dosáhnutí cílů,
- příležitosti – šance ke zlepšení,
- příkazy – nové požadavky vznesené vedením či regulatorními orgány apod.

Průběh každého projektu je dle autorky možné rozčlenit do několika částí – životní cyklus projektu je souborem jednotlivých projektových fází. Obvykle se jedná o návrh, plánování, implementaci a dokončení projektu. Obecně lze tyto první dvě fáze zaměřují na plánovací procesy a hovoří se o nich v souvislosti s proveditelností projektu. U druhé, realizační fáze se pak jedná o tzv. akvizici projektu. V souvislosti s informačními systémy je nutné hovořit i o životním cyklu produktu, resp. životním cyklu software. *„Mnoho informačních projektů zahrnuje průzkum, analýzu a následně nákup a instalaci nového hardwaru a softwaru bez potřeby realizace vlastního softwarového vývoje“* (Schwalbe, 2011).

Některé projekty však obsahují požadavek na modifikace softwaru a jiné jsou naopak téměř výlučně vývojové. Mezi známe modely životního cyklu vývoje systému (*Systems Development Life Cycle*, SDLC) patří spirálový model, vodopádový model, inkrementální přístup, prototypový přístup RAD (Rapid Application Development) nebo agilní metodiky (Scrum ad.) (Koch, 2010; Schwalbe, 2011).

V průběhu projektového řízení je také třeba správně odhadovat výši nákladů. Existuje několik typů odhadů prováděných v různých etapách životního cyklu projektu, které se vzájemně liší svojí přesností – např. hrubý odhad, rozpočtový odhad a konečný odhad. Tvorba rozpočtu spočívá v alokaci nákladů konkrétním položkám projektu v průběhu jeho trvání. Součástí řízení nákladů je sledování jejich efektivity a oznamování případných změn zainteresovaným stranám. Pro úspěch každého projektu má značný význam i řízení jeho kvality. Tu je nutné klást na stejnou úroveň, jako jsou další aspekty projektového trojimperativu (tj. rozsah, čas a náklady), jelikož je nezbytné zajistit, aby byl produkt ve shodě s požadavky a způsobilý k užívání tak, jak bylo na počátku projektu definováno. Řízení kvality projektu tak v praxi zahrnuje tři hlavní procesy – plánování kvality, zajištění kvality a kontrolu kvality. (Schwalbe, 2011) O kvalitě přitom nerozhoduje pouze kvalita produktu, resp. dodavatele, nýbrž i podmínky vytvořené na straně podniku, zvláště pak podpora na všech úrovních řízení. Uživatelé by měli mít dostatečné schopnosti a znalosti, mít dostatek času, a především ochotu změnit zavedené způsoby práce. Pro řídící pracovníky IT je nutná především schopnost komunikovat záměr s koncovými uživateli a dalšími osobami (Basl a Blažíček, 2012). O nedostatečné kvalitě některých IS/IT projektů se také hojně hovoří v médiích, zejména pak v souvislosti s tuzemskými státními zakázkami. Avšak problémy s rozsáhlými IT projekty nejsou jen ve veřejné sféře. Problémy IS/IT mohou vést nejen k rozsáhlým finančním ztrátám, ale mohou, v krajním případě, způsobit také ztráty na životech, jelikož informační systémy jsou do naší společnosti čím dál více integrované a na jejich správném fungování je závislých stále více odvětví a osob.

Schwalbe (2007) uvádí, že obdobně jako kvalitu je nutné v rámci realizace projektů řídit i obstarávání, integraci, rozsah a lidské zdroje (HR), jelikož lidé jsou významným aktivem společnosti. Mezi hlavní procesy řízení HR v projektech je vytvoření plánu HR, zajištění projektového týmu a jeho rozvoj a řízení. Významnou roli zde hrají především různé psychosociální faktory, jakými je například motivace pracovníků.

Efektivně řízení zaměstnanci mohou pracovat efektivněji a odvést nejlepší možnou práci v rámci daného projektu. Podobně důležitou složkou projektového řízení je komunikace, jejíž selhání představuje značnou hrozbu pro úspěch jakéhokoliv projektu. Informace je třeba vhodně distribuovat, což vyžaduje přípravu plánu komunikace s jednotlivými zainteresovanými stranami. Vhodně nastavenou komunikací je možno předcházet vzniku konfliktů a umožnit efektivně řešit konflikty (s časem, postupy, zaměstnanci apod.) již nastalé. Lidé mají často tendenci odporovat změnám spjatým se zavedením nového informačního systému či technologií, zvláště, jsou-li měněny jejich role v pracovním procesu. Molnár (2001) uvádí zejména následující důvody:

- komplexnost a rozsah změny,
- nedobrá historická zkušenost,
- nesprávné řízení procesu změny,
- nepochopení přínosů IS,
- neochota k experimentování,
- stávající psychosociální vazby na stávající procesy a řešení.

Tyto projekty se sebou nesou dle Molnára (2001) i další specifika, jelikož jsou povětšinou ovlivněny předchozími zkušenostmi, vyžadují sdílení podnikových zdrojů (zejména těch lidských) a probíhají simultánně s dalšími projekty (např. inovací procesů). Pro projekty podnikových informačních systémů je tedy typické, že postihují celou organizaci a přinášejí do podniku výrazný inovační potenciál s velmi krátkým cyklem změn. (Basl a Blažíček, 2012) Řízení projektů ve sféře IS/IT, resp. rozvoj IS/IT má svá specifika a je třeba o projektech rozhodovat v rámci informační strategie podniku, ze které by měly vycházet. V rámci ní tedy hledáme odpovědi na otázky týkající se prioritizace a etapizace projektů, dilemata týkající se nákupu vs. vlastního vývoje, revoluce vs. evoluce (zásadní změny či dílčí zlepšování) atd. Spadá sem i postavení útvaru informatiky v organizaci stejně jako přístup managementu k využívání IS/IT.

Obrázek č. 15: Hierarchická struktura řízení IS/IT
(Zdroj: vlastní zpracování dle Molnára, 2011)

Při postupu změny IS je nutné pro každou oblast změny realizovat následující kroky (Basl a Blažíček, 2012):

- provedení analýzy současného stavu,
- zpracování návrhu řešení,
- sestavení projektového plánu realizace,
- realizace projektu změny a uvedení do provozu,
- údržba a další rozvoj vč. aktualizace informační strategie.

Sodomka a Klčová (2010) rozdělují tento postup do šesti návazných etap. Prvotním krokem je dle nich provedení analytických prací a volba rozhodnutí (např. zda je potřeba nového IS nebo postačí inovovat stávající). Problematický je pak zvláště stav IS/ICT ve velkých organizacích či podnicích s více pobočkami, kde může paralelně existovat více různých dílčích IS a může být kvalitativně různá obsluha podnikových procesů. Druhým krokem je výběr systému (tj. produktu – HW, SW, infrastruktury, služby...) a implementačního partnera (dodavatele, systémového integrátora) a to obvykle formou výběrového řízení. Autoři zde akcentují nutnost minimální zakázkové úpravy (customizace), jelikož přinášejí časovou prodlevu a dodatečné náklady. Tento druhý krok povětšinou vyústí v uzavření smluvního vztahu s dodavatelem. Tato etapa patří mezi nejpodceňovanější a zároveň nejkritičtější místa. Poté nastává již samotná fáze implementace, která zahrnuje customizaci IS nebo jeho parametrizaci tak, aby co nejlépe odpovídal požadavkům podniku. V této fázi je také nezbytné započít se

školením uživatelů. Tuto fázi provází také častý vznik neočekáváných nadbytečných nákladů a časových prodlev, je tedy nutné klást vysoké nároky na dodržování harmonogramu. Předposlední fází je užívání a údržba systému, což je používání IS způsobem, který umožní realizaci očekávaných přínosů z jeho nasazení. Po této fázi následuje jeho rozvoj, inovace a to, co autoři označují jako „odchod do důchodu" – během této fáze jsou do podnikového IS integrovány další aplikace mající za úkol pokrýt klíčové procesy za účelem získání dodatečných přínosů. Způsob rozvoje IS je víceméně dvojí – buď je rozvíjen horizontálně, tedy zaměřen na spolupráci s dodavateli (SCM) či zákazníky (CRM) nebo vertikálně, tj. orientován na analytickou funkcionalitu (např. BI). Projektový záměr by měl vždy obsahovat všechny důležité charakteristiky plánovaného projektu, jakými jsou (Gála, Pour a Šedivá, 2015):

- důvody pro řešení, cíle a očekáváné efekty,
- cílové skupiny uživatelů,
- rozsah (jaké útvary),
- obsah (funkcionalita),
- vazby na jiné projekty nebo aplikace (a z toho plynoucí integrační řešení),
- kritické faktory (nároky), předpoklady a omezení,
- prioritizace částí,
- rámcový harmonogram,
- odhadovaná cena,
- základní vymezení nároků na řízení (organizace a role ze strany firmy).

Molnár (2001) definuje některé kritické faktory úspěchu projektů v oblasti IS/IT. K příčinám neúspěchu řadí zejména to, že:

- IS/IT nerespektuje organizační a vlastnické změny v podniku (nepočítá se změnou),
- dojde k podcenění zajištění konkurenceschopnosti (nezvládnutý rozvoj IS/IT),
- je malá angažovanost vrcholového vedení,
- chybí jednotná podniková informační strategie,
- je špatné řízení projektů (způsobující chybné časové i finanční odhady).

Časté chybné časové odhady, resp. opožďování a překračování plánovaných termínů zmiňují i Basl a Blažíček (2012). Časté je i překračování plánovaných nákladů a obtížné

sladění priorit a s tím i potřeby zdrojů. IS/IT musí být ve shodě jak s uživateli samotnými, tak s organizační i mocenskou strukturou a v neposlední řadě s okolním prostředím (Molnár, 2001). Pro úspěch projektu je dle Schwalbe (2007) stěžejní odhodlání organizace pro využívání informačních technologií v podniku a signifikantní podpora vedení dané organizace, které si musí uvědomit, že IS/IT je nedílnou součástí jejich podnikání a musí vytvořit ve vrcholovém managementu odpovídající pozici CIO (*Chief Information Officer*). Osoba CIO má v gesci přípravu informační strategie podniku a obvykle je zodpovědná za strategický rozvoj IS v podniku.

Jak již bylo zmíněno, mnoho projektů z oblasti IS/IT dle autorky nedodrží očekávaný rozsah, čas či náklady. Někteří manažeři uvádějí, že včasné dokončení projektu je jednou z největších výzev a současně hlavní příčinou konfliktů. Proto je nezbytně nutné věnovat zvláštní pozornost řízení času projektu. *„Čas je jednou z těch proměnných projektu, který jen nejméně flexibilní. Plyne bez ohledu na události, které v projektu nastanou“* (Schwalbe, 2011). Dle autorky mezi šest hlavních procesů patřících do řízení času spadá:

1. definování aktivit,
2. seřazení aktivit (a definování vztahů mezi nimi),
3. odhad zdrojů potřebných pro jednotlivé aktivity,
4. odhad doby trvání jednotlivých aktivit,
5. vytvoření harmonogramu,
6. kontrola harmonogramu.

Autorka dále uvádí, že harmonogram projektu vzniká na základě dokumentů, které byly vytvořené v první fázi projektu, tedy jeho zahájení. Seznam aktivit je tabulkový seznam činností obsahující jejich název, jednoznačný identifikátor a stručný popis. Atributy aktivity poskytují bližší informace – jako například předcházející a navazující činnosti, předpokládaná omezení a především – stanovená data trvání. Jako milník se pak označuje významná událost v projektu, která má obvykle nulovou délku trvání, avšak identifikuje nezbytné aktivity. Identifikované činnosti je nutné seřadit a definovat jejich vzájemné závislosti. K zobrazení souslednosti aktivit se používají například síťové grafy, které mohou být buď hranově orientované (aktivity jsou znázorněny šipkami) nebo uzlově orientované (aktivity znázorněny pomocí obdélníků). Pro vytvoření těchto

schémat je nutné odhadnout zdroje potřebné k zajištění jednotlivých aktivit tak, abychom posléze byli schopni odhadnout dobu trvání jednotlivých činností. Ze znázornění harmonogramu projektu se používá například Ganttových diagramů, analýzy kritické cesty (*Critical Path Method*, CPM) nebo analýzy PERT (*Program Evaluation and Review Technique*). Metody kritické cesty pomáhá předpovědět celkovou dobu trvání projektu, resp. nejdřívější možné dokončení projektu – jedná se o nejdelší cestu síťovým grafem, pokud se tedy zpozdí nějaká činnost na kritické cestě, zpozdí se i celý projekt. Technika PERT se používá v případech, kdy se pracuje s vysokou mírou nejistoty, jelikož využívá tří různých odhadů délky trvání Vážený průměr PERT je pak podíl součtu optimistického odhadu, čtyřnásobku nejpravděpodobnějšího odhadu a pesimistického odhadu času s číslem šest. Díky tomuto postupu výpočtu dob trvání aktivit se do odhadu celkové doby trvání projektu promítá i jisté riziko či nejistota jinak skrytá v jednotlivých dílčích odhadech. Posledním, ale neméně kritickým procesem řízení času projektu je kontrola harmonogramu, resp. kontrola jeho naplnění.

V souvislosti s projekty se hovoří také o využívání programů a řízení portfolií projektů. Program je skupinou souvisejících projektů, které jsou řízeny koordinovaně za účelem získání většího zisku a větší kontroly, což by při řízení každého samostatného projektu zvlášť nebylo možné. Seskupení více projektů tedy bývá ekonomičtější a pomáhá zefektivnit některé podnikové činnosti, jako je například řízení lidských zdrojů. Schwalbe (2011) uvádí některé typické programy v oblasti IT – infrastruktura, vývoj aplikací či uživatelská podpora.

2.12.1 Řízení a analýza rizik

Rizika jsou atributem většiny lidských aktivit, informační systémy a technologie nevyjímaje. Lidé, včetně manažerů, mají navíc rozdílný vztah k riziku – od averze až ke sklonům k riziku (Schwalbe, 2011; Veber a Srpová, 2012). Tyto tři typy preferencí rizika, resp. rizikového chování jsou součástí teorie užitku rizika. Užitek z rizika neboli tolerance k riziku představuje určité množství uspokojení z potenciálního přínosu rizika (Schwalbe, 2011). Pojetí rizika, a tudíž i jeho definice, je částečně odvislé od oboru. Obecně se riziko definuje jako nejistota, která může mít negativní či pozitivní vliv na splnění cílů projektu. Řízení pozitivních rizik v mnohém připomíná investiční

příležitosti (Schwalbe, 2011). Riziko může být však chápáno obecněji, jako (Fotr a Souček, 2011):

- možnost (či pravděpodobnost) vzniku ztráty,
- možnost výskytu událostí, které zabrání či ohrozí dosažení cílů,
- pravděpodobnost (nebezpečí) negativních odchylek od stanovených úrovní cílů.

Toto pojetí autorů nerozlišuje, zda se jedná o cíle jednotlivce, (investičního) projektu nebo organizace a je do značné míry oprávněné u těch rizik, která mají pouze negativní stránku (tzv. čistá rizika – *Pure Risk*). V podnikové praxi však obvykle převažují rizika podnikatelská, která mají také pozitivní stránku, a tudíž je i na pojetí rizika nahlíženo jinak (Fotr a Souček, 2011):

- variabilita možných výsledků,
- možnost odchylek (negativních i pozitivních) od očekávaných či plán. výsledků,
- pravděpodobnost výsledků odlišných od očekávaných (či plánovaných).

Je nutné odlišit vnímání rizika a nejistoty, byť i toto vnímání je do jisté míry závislé na oboru, ve kterém s těmito pojmy operujeme. *„Riziko je vždy spojeno s určitou akcí, aktivitou či projektem s nejistými výsledky, přičemž tyto výsledky ovlivňují situaci (často finanční) subjektu, který tuto akci realizuje. (...) Nejistota je pak spojena především s neschopností spolehlivého odhadu budoucího vývoje faktorů (faktorů rizika) ovlivňujících výsledky projektů (vývoj poptávky, prodejních cen, nákupních cen materiálů a energií, měnových kurzů, technologických změn aj.).“* (Fotr a Souček, 2011)

Riziko lze dělit podle nejrůznějších aspektů. Rizika IT projektu je možné kategorizovat dle nejrůznějších aspektů. Schwalbe (2007) je dělí do čtyř oblastí – obchodní rizika (tj. konkurence, dodavatelé, CF), technická rizika (tj. HW, SW, síťová), organizační rizika (tj. podpora vedení, podpora uživatelů, podpora týmu) a rizika řízení projektu (tj. odhady, komunikace, zdroje). Zvlášť důležité u projektů v oblasti IT je zapojení uživatelů, podpora vedení firmy a jasně definované požadavky. Fotr a Souček (2011) je pro změnu dělí na:

- systematické a nesystematické,
- vnitřní a vnější,
- ovlivnitelné a neovlivnitelné,

- primární a sekundární,
- ekonomická, výrobní, finanční, legislativní, politická, environmentální,…

Řízení rizik je tedy aktivita, jejímž primárním cílem je oslabení dopadu potenciálně nepříznivých událostí na projekt. Každý projekt obsahuje určitou míru nejistoty – klíč spočívá v nalezení rovnováhy mezi riziky a příležitostmi. Schwalbe (2007) uvádí, že se jedná o proces, v rámci kterého projektový tým průběžně identifikuje a analyzuje události, které mohou projekt negativně či pozitivně ovlivnit, stanovuje jejich pravděpodobnost a dopad a formuje reakci na rizika v průběhu celého jeho životního cyklu. Je esenciálně důležitým aspektem každého projektu výrazně zvyšující šance na jeho celkový úspěch. Správné řízení rizik může mít pozitivní dopad nejen na zpracování realistických odhadů časových plánů a nákladů, ale i na samotný výběr projektu a definici jeho rozsahu. Zapojuje také členy projektového týmu do procesu určování silných a slabých stránek projektu. Efektivní řízení rizik vede ke snížení výskytu problémů, a tedy i jejich rychlejšímu řešení, jelikož méně problémů je možné vyřešit rychleji. *„Na cíl řízení rizik lze pohlížet jako na minimalizaci potenciálních negativních rizik při současné maximalizaci potenciálních pozitivních rizik“* (Schwalbe, 2011).

Řízení rizik projektu se dle autorky skládá ze šesti hlavních procesů:

1. plánování řízení rizik,
2. identifikace rizik,
3. kvalitativní analýza rizik,
4. kvantitativní analýza rizik,
5. plánování reakcí na rizika,
6. monitorování a kontrola.

Autorka uvádí, že první krok zahrnuje rozhodování o přístupu k aktivitám řízení rizik v projektu. Projektový tým reviduje řízení nákladů, časový plán ad. Výstupem této fáze je plán řízení rizik. Druhým krokem je identifikace rizik neboli zjištění, která rizika mohou s určitou pravděpodobností ovlivnit realizaci projektu. Výstupem identifikace rizik je zejm. sestavení základní verze registru rizik, kde jsou zdokumentované vlastnosti každého z nich. Třetím krokem je kvalitativní analýza, která spočívá v seřazení rizik dle jejich závažnosti (na základě pravděpodobnosti výskytu a dopadu). Kvantitativní analýza obsahuje kvantifikující numerické odhady a stejně jako v případě

předcházejícího kroku je výstupem aktualizace stávajícího registru rizik. Pátým krokem je plánování reakcí na rizika, tedy takových kroků (opatření, protiopatření), které sníží pravděpodobnost či dopad jednotlivých rizik. Výstupem této fáze je, vyjma aktualizace registru, také aktualizování plánu řízení projektu i dalších projektových dokumentů. Posledním krokem je monitoring a kontrola spočívající v důsledném monitorování stávajících identifikovaných rizik včetně reziduálních a identifikaci rizik nových. V této fázi by se měly implementovat plány protiopatření a měla by se vyhodnocovat jejich efektivita. *„Je zřejmé, že kvalita přípravy ovlivňuje úspěšnost či neúspěšnost projektů zásadním způsobem, neboť nedostatky v přípravě vedoucí k volbě nevhodných projektů nelze obvykle odstranit, ale spíše oslabit v průběhu jejich realizace“* (Fotr a Souček, 2011).

Kvalitní příprava projektů, jejich hodnocení a výběr vyžadují dle Fotra a Součka (2011) identifikaci faktorů ovlivňující výsledky těchto projektů (tedy jejich úspěšnost), stanovení a zhodnocení dopadů těchto faktorů na budoucí výsledky projektů (tj. určení velikosti rizika) a zvážení možných opatření na snížení rizika. Souhrn těchto aktivit tvoří praktickou náplň managmentu rizik neboli risk managementu, jehož role je nedocenitelná zvlášť pak dynamickém podnikatelském prostředí plném nejistoty. Analýza rizik dle Smejkala a Raise (2013) zpravidla zahrnuje:

1. identifikaci aktiv – vymezení subjektu a popis aktiv,
2. stanovení hodnoty aktiv – na základě jejich významu a ohodnocení dopadu jejich ztráty, změny či poškození,
3. identifikace hrozeb a zranitelností – tj. událostí, které mohou negativně ovlivnit hodnotu aktiv a určení slabých míst, které umožní působení hrozeb,
4. stanovení závažnosti hrozeb a míry zranitelnosti – tj. pravděpodobnosti výskytu a zranitelnosti vůči dané hrozbě.

2.12.1.1 Identifikace a ohodnocení aktiv, hrozeb a zranitelností

Nejprve je nutné specifikovat pojem aktivum. Aktivum je všechno, co má pro subjekt (podnik) nějakou hodnotu a která může být zmenšena působením nějaké hrozby (Smejkal a Rais, 2013). Obecně lze aktiva dělit na hmotná a nehmotná, aktivem však může být i subjekt samotný. Základní charakteristikou aktiva je jeho hodnota, která je jednak objektivní (tj. cena či náklady na překlenutí případné škody na aktivu, případně

určité výnosové charakteristiky), ale jednak také na subjektivním ohodnocení kritičnosti aktiva pro daný subjekt. Proto je hodnota aktiva relativní v závislosti na úhlu pohledu, typické je to zvláště u informačních aktiv. Hrozba je definována jako *„síla, událost, aktivita nebo osoba, která má nežádoucí vliv na bezpečnost nebo může způsobit škodu“*. Hrozby jsou charakterizovány svojí nebezpečností, přístupem a motivací. Dopadem hrozby je škoda, kterou svým působením na aktivum způsobí. Zranitelnost je slabina, nedostatek nebo stav aktiva, kterého může být využito hrozbou. Zranitelnost tedy popisuje, jak citlivé je aktivum na působení dané hrozby. Úroveň zranitelnosti je možné vyjádřit pomocí citlivosti a kritičnosti. Protiopatření je pak postup, proces nebo technický prostředek navržený pro zmírnění působení hrozby či její úplnou eliminaci. Protiopatření je vždy charakterizováno efektivitou a náklady. Náklady na protiopatření by pochopitelně neměly přesáhnout hodnotu chráněného aktiva. Autoři dále uvádějí, že identifikace aktiv spočívá ve vytvoření soupisu veškerých aktiv, které spadají do analýzy rizik. Je třeba brát v úvahu jejich případnou nahraditelnost a jedinečnost. Aktiv je obvykle velmi velké množství, což vede ke seskupování podobných aktiv do skupin s podobnými vlastnostmi (cena, účel atp.). Každá hrozba se vždy hodnotí vůči každému aktivu či jejich skupině. (Smejkal a Rais, 2013)

2.12.1.2 Identifikace rizik

Identifikace rizik představuje proces, jehož účelem je rozpoznat potenciální situace, jež mohou daný projekt poškodit (popř. vylepšit). Potenciální rizika je nutné identifikovat co nejdříve, avšak ani v průběhu realizace projektu se na rozpoznávání rizik nesmí zapomenout. Je nutné mít na paměti, že neidentifikovaná rizika není možno řídit. Již identifikovaná a analyzovaná rizika se označují jako známá rizika – tyto lze proaktivně řídit na rozdíl od neznámých, která již z podstaty věci řízena být nemohou. (Schwalbe, 2011)

Projektové týmy proces identifikace rizik dle autorky často zahajují revizemi projektové dokumentace, zvláště pak sběrem informací, např. pomocí týmového brainstormingu, metody Delphi, realizací rozhovorů nebo SWOT analýzou. Jak již bylo řečeno, hlavním výstupem této fáze řízení rizik je zpracování tzv. registru rizik, což je dokument, nejčastěji tabulka, kde je uveden výčet potenciálně rizikových (avšak nejistých) situací či událostí jejichž vznik může ovlivnit projekt. V registru může být uvedena kupříkladu

kategorie rizika (například viz. oblasti výše), spouštěče dané rizikové události (např. překračování nákladů hned zpočátku) a specifikace vlastníka rizika, tj. osoby, která převezme za riziko odpovědnost. V registru rizik je možné uvádět i stav rizika, zda například došlo k přijetí nějakého opatření. Systematická revize jednotlivých evidovaných rizik pomáhá udržovat registr rizik stále aktuální.

Fotr a Souček (2011) uvádějí, že cílem identifikace rizik je získání souboru faktorů, které by mohly ovlivnit dosažení cílů projektů a tím i jejich úspěšnost. Samotná identifikace rizik vyžaduje určité vstupy, použití vhodných metod a nástrojů a zapojení pracovníků, kteří disponují potřebnými informacemi o projektu a jsou na jeho výsledcích zainteresování. Identifikace rizik je kolektivní záležitostí a je nanejvýš vhodné vytvořit pro tyto účely tým, kde by měli být zastoupeni zejména členové projektového týmu (kteří se podílejí na přípravě a plánování projektu), specialisté z oblasti projektu (interní či externí) a stakeholdeři. Při sestavování seznamu rizik je nutné důkladně jeho prověření tak, aby se zamezilo duplicitě rizik a aby se neevidovala rizika, která nejsou riziky (protože se jedná o situace existující s jistotou) stejně jako rizika, která neovlivňují dosažení cílů projektu (tj. irelevantní rizika). Je také vhodné specifikovat jednotlivá rizika v podobě vztahu příčin a následků, mohou se tak například identifikovat společné příčiny.

2.12.1.3 Hodnocení rizik

Výsledkem identifikace rizik je dle autorů obvykle větší množství rizikových faktorů, které je nutné určitým způsobem kategorizovat, jelikož zpravidla není možné věnovat stejnou pozornost všem těmto faktorům, a tedy ani připravit opatření na snížení rizika. Ke stanovení významnosti rizik lze využít buď analýzu citlivosti (za předpokladu, že existují kvantifikovatelná rizika a lze tedy modelovat závislost kritérií hodnocení na faktorech rizika) nebo expertní hodnocení, jehož nástrojem je zejm. matice hodnocení rizik, která se používá u obtížně kvantifikovatelných nebo nekvantifikovatelných rizik. (Fotr a Souček, 2011) Jedná se o matici či diagram, který má na jedné ose dopad rizika a na druhé pravděpodobnost jeho výskytu, resp. vzniku. Matici je možné ještě rozdělit do devíti kvadrantů dle míry pravděpodobnosti a dopadu (vysoká/vysoký, střední/střední, nízká/nízký) (Schwalbe, 2011).

Princip matice hodnocení rizik spočívá v ohodnocení těchto rizik pracovníky, kteří mají potřebné znalosti a zkušenosti v oblastech, kam jednotlivá rizika spadají. Identifikovaná rizika se posuzují ze dvou hledisek – pravděpodobnosti výskytu rizika a intenzity dopadu tohoto rizika. Riziko, resp. faktor rizika je tím významnější, čím pravděpodobnější je jeho výskyt a čím vyšší je intenzita jeho dopadu v případě jeho výskytu. Povětšinou má toto hodnocení formu kvalitativního hodnocení, byť se lze setkat i s vyšší formou tohoto hodnocení, tzv. semikvantitativním hodnocením. (Fotr a Souček, 2011) *„Některé projektové týmy vypočítávají ke každému riziku jediné číselné skóre, které vznikne vynásobením číselného skóre pravděpodobnosti a číselného skóre dopadu. Mnohem sofistikovanějším postupem je využít informace o pravděpodobnosti a dopadu k výpočtu rizikových faktorů – jde o veličiny, které vyjadřují celkové riziko konkrétních událostí při dané pravděpodobnosti jejich výskytu a důsledků pro projekt ve chvíli, kdy nastanou.“* (Schwalbe, 2011)

V základní formě hodnocení se operuje obvykle pouze s negativními dopady a pětistupňovou stupnicí. Mimo ohodnocení samotných rizik je nutné při hodnocení rizika projektu zvažovat i další významné faktory vztahující se k projektu, jako je například jeho rozsah a izolovanost, informace o realizaci obdobných projektů konkurencí, riziková kapacita a z ní vyplývající velikost tolerovaného rizika atd. (Fotr a Souček, 2011) V některých projektech postačuje provedení kvalitativní analýzy, nicméně mnohdy následuje po jejím provedení analýza kvantitativní. Konkrétní typ prováděné analýzy závisí především na povaze projektu a zahrnuje často modelování, simulace (např. Monte Carlo) a analýzy citlivosti. (Schwalbe, 2011)

Pro udržení povědomí o rizicích po celý životní cyklus projektu je možné použít metodu sledování deseti nejzávažnějších rizik, jejíž součástí je zavedení pravidelných revizí nejzávažnějších rizik. Tyto revize naplňují hned několik cílů – management podniku (případně i zákazník) jsou pravidelně informováni o zásadních vlivech, které projekt ovlivňují a při zapojení zákazníka může projektový tým zvažovat i alternativní způsoby řešení rizik. (Schwalbe, 2011) Vyhodnotíme-li nějaké riziko jako přijatelné, obvykle není nutné plánovat protiriziková opatření a projekt může být realizován beze změny – jedná se o tzv. retenci (zadržení) rizika. Je-li riziko vyhodnoceno jako nepřijatelné, může přijít v úvahu buď vyhnutí se riziku nebo volba strategie vedoucí ke snížení rizika. (Fotr a Souček, 2011)

2.12.1.4 Opatření

Výsledkem identifikace rizik a jejich ohodnocení by mělo být naplánování protirizikových opatření. Primárním cílem těchto opatření je přispět k ekonomicky účelnému snížení rizika projektu (tedy nikoliv minimalizace rizika za každou cenu) vyvolanému hrozbami a posílit příležitosti s jejich pozitivními dopady na projekt. Do náplně plánování protirizikových opatření patří dle Fotra a Součka (2011) zejména:

- zvažování všech rizik projektu identifikovaných jako významné,
- volba vhodné strategie,
- příprava samotných protirizikových opatření.

Základní strategie snižování rizika spočívá v oslabení (či eliminaci) příčin vzniku rizika, vedoucí ke snížení pravděpodobnosti výskytu negativních rizik (tj. prevence rizika), dále ve snižování negativních dopadů rizik nebo transferu rizika na jiné subjekty (Fotr a Souček, 2011). Schwalbe (2011) uvádí čtyři základní strategie, kterými lze reagovat na negativní rizika:

- vyhnutí se riziku – tj. eliminace konkrétní hrozby obvykle potlačením její příčiny,
- akceptace rizika – tj. přijetí důsledků,
- transfer rizika – tj. přenos důsledků a odpovědnosti na třetí stranu,
- zmírnění rizika – tj. snížení dopadu pomocí snížení pravděpodobnosti výskytu.

Obdobně jako negativní, tak i pozitivní rizika je možné podpořit čtyřmi základními strategiemi – jejich využitím, sdílením, posílením či pouhým přijetím. V oblasti IT ilustruje Schwalbe (2011) vyhnutí se riziku na výběru známého hardwaru či softwaru v novém projektu na základě předchozích zkušeností. Určitou formu akceptace rizika může být příprava alternativních či záložních plánů („plán B “) nebo tvorba rezerv na mimořádné události. Transfer rizika lze nejlépe ilustrovat na principu pojištění nebo aplikování rozšířené záruky na hardware. Zmírněním rizika může pak být například zapojení zkušených pracovníků nebo aplikace různých validačních technik. O pozitivních rizicích se v souvislosti s IT projekty hovoří zejména o pozitivním PR.

Opatření je tedy, obdobně jako strategii snižování rizika, možno dle Fotra a Součka (2011) dělit například na:

- Opatření orientovaná na příčiny rizika,
    - uplatňování nástrojů řízení
    - změny procesů
    - vertikální integrace
- Opatření orientovaná na oslabení nepříznivých dopadů rizika,
    - diverzifikace
    - sdílení rizika
- Transfer rizika
    - pojištění.

Při výběru protirizikových opatření je nutné akcentovat ekonomickou efektivnost navrhovaných opatření (tedy relaci snížení rizika k vynaloženým nákladům) a sekundární rizika, tedy že realizace protirizikového opatření může vyvolat jiná rizika – např. přidáním nového hardwaru do systému nastane nutnost rekonfigurovat software. Z dalších kritérií je možné jmenovat např. dostupnost zdrojů a obtížnost implementace daného opatření. Výsledné riziko, tj. po realizaci opatření, se označuje jako reziduální (netto, zbytkové) riziko – může jít např. o určité riziko poruchy zařízení (Schwalbe, 2011). Velikost dopadů rizik bude také záviset na pohotovosti a konkrétní reakci podniku na rizikovou situaci (Fotr a Souček, 2011). Účinným nástrojem je včasná příprava plánů havarijních (korekčních) opatření – např. *Business Continuity Plan* (BCP) nebo *Disaster Recovery Plan* (DRP). Veškerá identifikovaná a ohodnocená rizika a navržená opatření by pak měla být soustředěna v podobě určitého registru či databáze rizik. Je třeba mít na paměti, že řízení rizik je kontinuální proces. V průběhu celého životního cyklu projektu je nutné sledovat a vyhodnocovat rizika na základě stanovených milníků a přijímat rozhodnutí, resp. realizovat opatření související s riziky.

„Řízení rizik nekončí počáteční analýzou rizik. Rizika, která tým identifikoval, se nemusí vůbec objevit nebo se pravděpodobnost jejich vzniku či dopad může snížit, případně zcela zmizet. Naopak u dříve definovaných rizik můžete zjistit, že jsou jejich pravděpodobnost či odhadové ztráty vyšší. Obdobně můžete při realizaci projektu identifikovat rizika nová.“ (Schwalbe, 2011) Mezi nástroje pro monitoring rizik je

možné, vyjma jejich opakovaného hodnocení, řadit též analýzy trendů a odchylek či pravidelné revize.

2.13 Analytické metody, nástroje a modely

V této části práce jsou vysvětleny analýzy vnitropodnikové stejně jako analýzy vnějšího podnikového prostředí. Objasněny jsou také některé metody a modely vztahující se k problematice podnikových informačních systémů.

2.13.1 SWOT analýza

Analýza SWOT (*Analysis of the Strengths and Weaknesses of an organization and the Opportunities and Threats facing*), tedy analýza silných a slabých míst organizace a příležitostí a hrozeb, kterým je organizace vystavena, slouží jako jedna ze základních strategických analýz (Synek et al., 2001). Silná a slabá místa vychází zevnitř podniku a příležitosti a hrozby jsou identifikovány ve vnějším okolí podniku. Je nutné ohodnotit jejich dopad na podnikovou strategii. SWOT analýza je tedy užitečným pohotovým nástrojem k popisu celkové situace podniku (Váchal a Vochozka, 2013).

Účelem SWOT analýzy je především vyzdvihnutí těch stránek, jež mají strategický význam. Je také nutné identifikované stránky prioritizovat, jelikož některá zjištění jsou důležitější nežli ostatní, protože jejich vliv na trh je silnější a při realizaci dané strategie hrají rozhodující roli (Váchal a Vochozka, 2013). Závěry SWOT analýzy by tedy měly být vždy vztažené ke konkrétní situaci podniku. Této analýze se často podrobuje celý podnik a zkoumá se (obvykle v týmu) výrobky, marketing, finance, řízení podniku, konkurenci ad. Výsledkem jsou obvykle nové plány, které zabezpečí splnění cílů firmy (Synek et al., 2001).

Z analýzy vzejdou čtyři typy strategie na základě jejich interakcí. Tyto, z analýzy vzešlé, strategie jsou často označovány např. „ S_2O_4 “ , aby odkazovaly na jednotlivé zjištěné silné a slabé stránky, příležitosti a hrozby. Váchal a Vochozka (2013) specifikují, že se jedná o:

- S-O strategie (tj. využití – využití silných stránek ke zhodnocení příležitostí),
- W-O strategie (tj. hledání – překonání slabých stránek využitím příležitostí),
- S-T strategie (tj. konfrontace – využití silné stránky k odvrácení ohrožení),

- W-T strategie (tj. vyhýbání – minimalizace slabé stránky a zároveň vyhnutí se ohrožení).

Dle autorů je strategie S-O je spíše žádoucím stavem, ke kterému podnik směřuje, jelikož příležitosti tohoto typu nejsou v podnikové praxi příliš častým jevem. Strategie S-T mají veskrze pozitivní dopad na podnik, obdobě jako W-O , avšak pouze za předpokladu, je-li podnik dostatečně silný na přímou konfrontaci. W-T strategie jsou ryze obrannými strategiemi a podnik v této situaci obvykle bojuje o své přežití.

2.13.2 SLEPTE analýza

SLEPTE (STEP, PEST, PESTEL ad.) analýza je relativně jednoduchým, a přesto efektivním nástrojem k ohodnocení vlivu faktorů globálního prostředí, tj. externích faktorů, působících na podnik. Výstupem této analýzy je nalezení odpovědí na následující otázky ve vzájemně se ovlivňujících segmentech vnějšího prostředí (viz. název) (Váchal a Vochozka, 2013):

- Které externí faktory mají vliv na podnik?
- Jaké jsou jejich možné účinky?
- Které z nich jsou (v nejbližší budoucnosti) nejdůležitější?

Tato analýza existuje v několika modifikacích dle rozsahu zkoumaných faktorů, povětšinou však zkoumá následující vlivy vnějšího prostředí:

- Sociální (resp. Sociálně-kulturní) – demografie, mobilita, vzdělání,
- Legislativní – platné i připravované zákony, daňová politika,
- Ekonomické – trend vývoje HDP, úroková míra, inflace, cena energií,
- Politické – situace na politické scéně, stabilita vlády, míra korupce,
- Technologické – nové objevy, vynálezy, patenty, výdaje na VaV,
- Environmentální – ochrana životního prostředí.

Výhodou SLEPTE analýzy je dle autorů zaměření se na širší podnikové prostředí, resp. jeho změny, které nemusejí být při zkoumání odvětví na první pohled patrné. Tento nástroj také kalkuluje i s neekonomickými faktory, nicméně ne vždy jeho použití přinese nová zjištění.

2.13.3 Porterův model pěti sil

Porterův model vychází z principu, že každé odvětví je možno charakterizovat pomocí určitých ekonomických a technických faktorů, které jsou základem konkurenčních sil. Stav konkurence dle Porterova modelu závisí na působení pěti základních sil, přičemž výsledkem jejich společného působení je ziskový potenciál odvětví. Předností tohoto modelu je jeho analytická systematičnost, s níž prezentuje tvorbu konkurenčních sil – umožňuje nám určit jaké jsou konkurenční tlaky, odkud tyto tlaky pocházejí a jak se proti nim bránit, popř. jak se na ně adaptovat. Celkový dopad konkurenčních sil působících na podnik ovlivňuje vznik specifického druhu konkurence na trhu a v konečném důsledku tak determinuje zisky, kterých mohou podniky dosáhnout. *„Je pravidlem, že se celková ziskovost podniků v odvětví snižuje, když se konkurence stává aktivnější. (...) Na druhé straně, když odvětví nabízí perspektivu vysoké a dlouhodobé ziskovosti, lze usoudit, že konkurenční síly nebudou nadmíru silné a že konkurenční prostředí v daném odvětví bude příznivé a atraktivní.“* (Váchal a Vochozka, 2013)

Aby se podnik s vlivem konkurence, resp. konkurenčních sil vyrovnal, je třeba, aby zaujal na trhu nejméně zranitelnou pozici a zvolil takový přístup ke konkurenci, který mu poskytne nejlepší možnosti obrany, tj. umožní mu se co nejvíce izolovat od působení konkurenčních sil a využívat existující odvětvové konkurenční síly ve svůj prospěch. Pro podnik je výhodné, pokud dokáže zaujmout takovou pozici, která mu umožní „rozehrát hru“ ihned, jak se nějaká konkurence v jeho odvětví objeví. Při aplikaci Porterovy analýzy je nutné ohodnotit všech pět následujících konkurenčních sil (Váchal a Vochozka, 2013):

- rivalita mezi existujícími podniky,
- ohrožení ze strany nových konkurentů,
- vyjednávací síla dodavatelů,
- vyjednávací síla odběratelů,
- ohrožení substituty.

Autoři dále uvádějí, že rivalita mezi již existujícími podniky, tedy stávající konkurencí, je důsledkem přirozené snahy každého podniku zlepšit vlastní pozici. Rivalita obecně narůstá, pokud jsou konkurující si podniky početné a přibližně stejně velké, fixní náklady jsou vysoké a je nízký stupeň diferenciace produktu, stejně jako pokud je míra

růstu odvětví nízká a zvýšení podílu na trhu je tak možné pouze na úkor konkurence. Míra ohrožení ze strany nových konkurentů značně závisí na bariérách vstupu do odvětví a reakci etablovaných podniků na vstup nové konkurenčního organizace. Zavedené podniky mohou, mají-li dostatečné finanční zdroje, odvrátit vstup nových konkurentů do odvětví. Bariéry vstupu do odvětví jsou spjaty zejména s existencí úspor z rozsahu, které favorizují velké a na trhu etablované podniky. Nejde přitom pouze o samotný rozsah výroby, ale také marketing, R &D apod., což mj. zhoršuje přístup k distribučním kanálům. Bariéry vstupu tvoří také kapitálová náročnost některých odvětví, diferenciace výrobků (silné značky, loajální zákazníci), ale také vládní politika – například regulace některých odvětví a s tím spjaté licenční požadavky nebo limity environmentálního rázu (např. emisní limity elektráren). Bariérou mohou být i různá nákladová znevýhodnění, která nemusejí přímo souviset s velikostí podniku – zavedené podniky mají obvykle určité výhody oproti nově příchozím například v podobě výhodnějšího umístění, v přístupu k surovinovým zdrojům nebo získání vládních dotací. Vyjednávací síla dodavatelů spočívá zejména v možnosti zvýšení cen, popř. snížením kvality dodávaných produktů. Vyjednávací síla dodavatelů je závislá zejména na stupni jejich koncentrace, diferencovanosti produktu (nese-li sebou vysoké náklady na změnu dodavatele) a vázanosti na dodávkách z jiných odvětví. V případě vyjednávací síly odběratelů, je zde, podobně jako u dodavatelů, možnost výrazně ovlivnit svým tlakem cenu či kvalitu produktů v odvětví. I zde má vliv stupeň koncentrace (velcí odběratelé mají silnou pozici zejména vůči podnikům s vysokými fixními náklady), míra diferenciace, zisk na odběrateli nebo cenová senzitivita. Jak u dodavatelů, tak u odběratelů je zde také otázka možnosti vertikální integrace. Co se týká ohrožení substituty, obecně platí, že čím snazší je nahrazení produktu substituty, tím je dané odvětví méně atraktivní. Strategicky důležitými substituty jsou pak zejména ty vyráběné v ziskovějších odvětvích nebo ty, které technologickými inovacemi dokáží nabídnou lepší uspokojení potřeb.

Porterův model je možno využít i ve vztahu k informačním systémům, resp. informačním technologiím – přináší tak známých pět oblastí, které jsou však zaměřeny a aplikovány ve vztahu k IS/IT (Molnár, 2001; Basl a Blažíček, 2012):

- současná konkurence na trhu (Může IS/IT pomoci vytvořit konkurenční výhodu?),

- hrozba vstupu nových konkurentů (Může IS/IT pomoci vybudovat bariéry vstupu?),
- hrozba vstupu substitučních produktů (Může IS/IT pomoci vytvářet nové produkty?),
- vyjednávací síla dodavatelů (Může IS/IT pomoci změnit jejich vyjednávací sílu?),
- vyjednávací síla odběratelů (Může IS/IT pomoci změnit jejich vyjednávací sílu?).

Základním výstupem modelu je dle Molnára (2001) zodpovězení otázky, jak nám může pomoci IS/IT pomoci vytvořit výhodu vůči konkurenci, resp. jaká aplikace zmírní či odstraní některou z hrozeb (např. vstup nových konkurenčních subjektů na trh). Hrozbě současné konkurence, resp. stávajících konkurenčních subjektů se lze bránit v zásadě třemi základními způsoby – strategií nízkých nákladů, odlišením se nebo nalezením mezery na trhu.

2.13.4 McKinsey 7S

McKinseyho model slouží ke strategické analýze interních faktorů, resp. pro hodnocení kritických prvků představujících nutnou podmínku pro úspěch organizace při realizaci její podnikové strategie. Mezi hlavní faktory úspěchu patří strategie, struktura podniku, spolupracovníci a jejich schopnosti, styl řízení firmy, systémy a sdílené hodnoty (Smejkal a Rais, 2013).

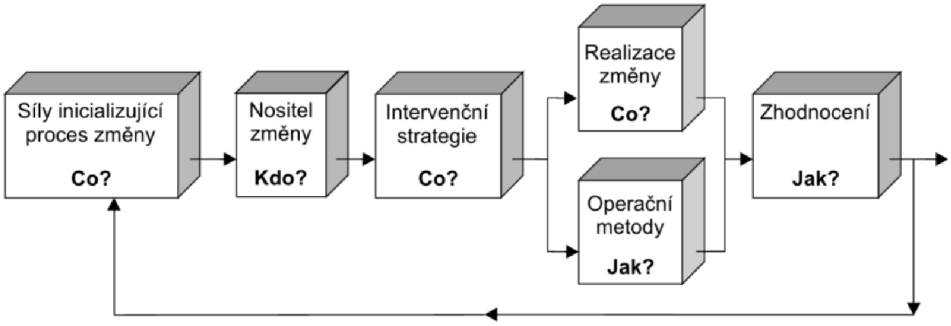
Autoři uvádějí, že strategie obvykle vychází z vize a poslání daného podniku a je charakterizována dlouhodobým zamýšleným směřováním firmy k jednomu cíli či množině cílů. Jedním z těchto elementárních podnikových cílů je například dosažení určité konkurenční výhody a uspokojení očekávání stakeholderů. Co se týče strategie je nutné si uvědomit, že nejde jen o její prezentaci, ale především o její realizaci, naplňování a posléze její vyhodnocování. V podniku obvykle existuje hierarchie strategií, na jejímž vrcholu je tzv. corporate strategie, která určuje základní orientaci podniku na tuto strategie navazuje business strategie a na nejnižší úrovni jsou pak tzv. funkční strategie – např. marketingová nebo výrobní. Dle Porterova pojetí obecně existují dvě základní konkurenční výhody – nízké náklady nebo diferenciace (produktů či služeb).

Dle autorů slouží organizační struktura k optimálnímu rozdělení kompetencí a pravomocí. Rozlišuje se několik základních typů organizační struktury – liniová (tj. jeden útvar nadřazen ostatním), funkcionální (tj. několik vedoucích dle funkce), maticová (prvky jak funkcionální, tak divizionální), liniově štábní (tj. jedno vedení a funkcionální struktura), divizionální (tj. relativně samostatné divize) atd. Často nelze identifikovanou podnikovou strukturu jednoznačně zařadit do výše uvedených kategorií a hovoří se o tzv. hybridních strukturách. Spolupracovníci, tedy zaměstnanci a pracovníci jsou hlavním zdrojem zvyšování produktivity podniku, avšak také značným provozním rizikem. Je nutné je motivovat a zvyšovat atraktivnost podniku, k čemuž pomáhá i cílená tvorba firemní kultury nebo třeba otevřená komunikace. Jak uvádí Rais, nezastupitelnou roli zde hrají tzv. mistři změny, což jsou tvůrčí vedoucí pracovníci – lídři, kteří se stávají hybnou silou inovačního úsilí. Schopnosti, zvláště manažerů, musí odpovídat často uváděným charakteristikám a vlastnostem úspěšného manažera, jako je například výkonnost, schopnost motivovat a vhodně odměňovat, komunikační schopnosti apod. Zvláště ceněná je schopnost rychle se adaptovat. Styl řízení obvykle odpovídá klasické typologii, resp. dělení na autoritativní, demokratický (obousměrná komunikace, větší angažovanost pracovníků) a laissez-faire (či liberální). Systémy jsou určité formální mechanismy pro měření, odměňování a alokaci zdrojů. Příkladem mohou být např. informační systémy, které mohou být formalizované i neformalizované a dle toho se i liší míra automatizovanosti zpracování informací. Sdílené hodnoty souvisí úzce s oblastí spolupracovníků, jelikož se prakticky jedná o souhrn přístupů a hodnot, jež jsou v organizaci dlouhodobě udržované a panuje o nich obecné povědomí.

2.13.5 Lewinův model

Rozhodne-li se podnik ke změnám, dle Smejkala a Raise (2013) je nutné provést analýzu sil, které působí pro a proti změně a je nezbytné identifikovat agenta změny, jenž bude realizátorem celého procesu. Může se jednat o jednotlivce nebo skupina pracovníků, kteří budou nositeli změny. Tento agent změny bude podporován jejím sponzorem, což je obvykle majitel společnosti. V rámci realizace procesu změny hraje významnou roli flexibilita zaměstnanců a jejich ochota změnu akceptovat. Zásadní význam pro změnu má nespokojenost zaměstnanců se současným stavem a zároveň míra osobního rizika plynoucího ze změny – s tímto vědomím je možné zaměstnance

kategorizovat do několika skupin a přizpůsobit tak komunikaci se zaměstnanci či jejich motivaci, což v důsledku vede ke snížení rizika neúspěchu celého projektu. V zaměstnancích je potřebné vyvolat pocit potřeby změny, musí se zjistit jejich očekávání a požadavky, ukázat, že neutrpí ztrátu. Dát jim čas na osvojení si změny. Zkrátka je třeba brát v úvahu i psychosociální, resp. kulturní a lidské aspekty celé změny. *„Překonání odporu lidí k implementačním projektům a jejich aktivní zapojení do procesu změn patří ke klíčovým problémům budování informačního systému. Proto je žádoucí pojmout realizaci IS/ICT komplexně a využít přitom některý z modelů řízení změny.“* (Sodomka a Klčová, 2010) Následně je nutné identifikovat tzv. intervenční oblasti, tedy oblasti, do kterých budou směřované změnové zásahy (Smejkal a Rais, 2013).



Obrázek č. 16: Lewinův model řízené změny
(Zdroj: Smejkal a Rais, 2013)

Smejkal a Rais (2013) specifikují následující intervenční oblasti:

- Lidské zdroje a jejich řízení,
- Organizační struktura firmy,
- Technologie firmy,
- Komunikační a organizační toky a procesy.

Lewinův model vychází z principu, že změna vyžaduje posun od statického stavu přes provedenou aktivitu k dalšímu statickému stavu. Fáze v tomto třístupňovém procesu jsou následující (Sodomka a Klčová, 2010):

- rozmrazení,
- změna,
- opětovné zmrazení.

První krok, tedy rozmrazení, zahrnuje vytvoření „stavu nespokojenosti“, který tvoří podmínky k uskutečnění změny vč. analýzy všech aspektů nutných k provedení samotné změny. Jak již bylo zmíněno, je nutné vést informační kampaň mezi zaměstnanci. Následně je možné realizovat vlastní intervenci – vlastní plánovanou změnu – vlastní projekt. Třetí fází je opětovné zmrazení, tedy ukotvení a stabilizaci nového stavu v podniku. Tento model příliš neakcentuje evoluční vývoj, jelikož často bývá výchozím bodem v podniku situace, kde je prostředí nestabilní a nepředstavuje tedy statickou entitu. (Sodomka a Klčová, 2010) Na závěr je nutné verifikovat dosažené výsledky. V případě kvantitativních parametrů je vyhodnocení úspěšnosti projektu pochopitelně podstatně snazší nežli v případě kvalitativních.

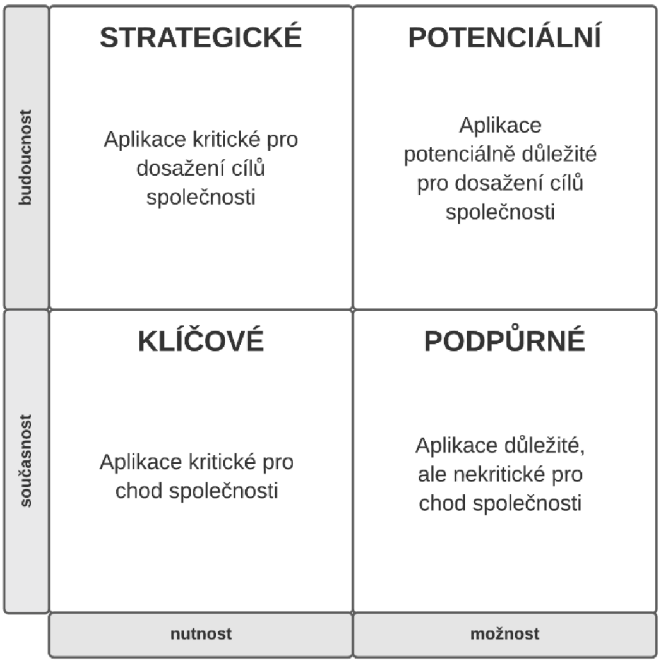
Lewinův model je někdy podrobován kritice zejména pro svoji statickou povahu a fakt, že se v praxi dost často jednotlivé jeho fáze vzájemně prolínají (Smejkal a Rais, 2013). Existují i další modely řízení změn – od relativně jednoduchých až po komplexnější. Sodomka a Klčová (2010) uvádějí například Model plovoucího ledovce, jenž vychází z technokratického pohledu manažerů na řízení změny a opírá se o projektový trojimperativ, který tvoří pověstnou špičku ledovce. Pod „hladinou“ však existují další dvě dimenze, a to řízení vnímání a řízení síly a zájmů, kalkuluje tedy s předpokládanými bariérami. Samotná strategie změny je pak buď skoková, revoluční transformace nebo inkrementální, evoluční vylepšování. Model plovoucího ledovce v sobě více akcentuje sociální aspekty změny a rozlišuje čtyři skupiny lidí: oponenty, příznivce, skryté oponenty a potenciální příznivce.

2.13.6 Analýza stakeholderů

Analýza stakeholderů neboli analýza zainteresovaných stran je postup používaný pro řízení projektů. Jedná se o identifikaci a analýzu subjektů, které jsou buď do projektu přímo zapojeny, nebo jejichž zájmy jsou přímo či nepřímo ovlivněny jeho realizací. Stakeholdeři také často mohou výrazně ovlivnit průběh celého projektu. (Doležal, Máchal a Lacko, 2012) Cílem analýzy je posouzení tohoto ovlivnění za účelem úpravy strategie pro jednání s jednotlivými zainteresovanými stranami. K popisu stakeholderů, resp. jejich vlastností je možné využít celé řady kritérií. Podle jejich vlivu a zájmu lze posléze rozdělit zainteresované strany například od matice vlivu a zájmu, což usnadňuje následné použití v řízení zainteresovaných stran.

2.13.7 McFarlanův model aplikačního portfolia

Model portfolia aplikací rozvádí přínosy jednotlivých aplikací pro podnik z pohledu jejich důležitosti (resp. naléhavosti) a současnosti i budoucnosti, čímž do určité míry postihuje i princip postupné výstavby informačních systémů v podnicích (Molnár, 2001). Svým principem navazuje na tzv. Bostonskou matici. Toto rozřazení aplikací podnikových informačních systémů napomáhá rozlišit časovou základu pro zohlednění investic do IS stejně jako napomáhá postupnému budování IS s ohledem na potřeby podniku dané jeho podnikatelskou činností na straně jedné a aktuálními možnostmi ICT na straně druhé (Basl a Blažíček, 2012). Vlastní portfolio aplikací by měl každý podnik sledovat, a zvláště pak neopomínat oblast aplikací zaměřených do budoucna, protože právě tyto aplikace mohou v budoucnu přinést podniku konkurenční výhodu.



Obrázek č. 17: McFarlanův model aplikačního portfolia
(Zdroj: vlastní zpracování dle Molnára, 2011)

Podpůrné aplikace se orientují na samotný chod podniku (mohou např. umožňovat snižování nákladů), jsou pro něho důležité, avšak ne nezbytně nutné (kritické) a jejich přínosy jsou povětšinou realizovatelné v relativně krátkém horizontu (a taktéž měřitelné). Basl a Blažíček (2012) mezi podpůrné aplikace řadí například účetnictví nebo mzdy). Klíčové aplikace jsou taktéž orientovány na současnost a realizovatelné v krátkém horizontu. V podniku jsou klíčové aplikace nejvýraznější v případě, že dojde

k potížím s jejich funkčností – jejich paralýza může totiž vést až k zastavení provozu podniku. Jejich přínosy jsou navíc měřitelné pouze částečně. V praxi se dle Basla a Blažíčka (2012) jedná například o řízení výroby nebo řízení skladových zásob.

„Omezení stávajících informačních systémů a orientace pouze na tzv. podpůrné aplikace a úmyslné přehlížení tzv. strategických či potenciálních aplikací u převážné většiny dnešních firem proto silně limituje proces uskutečnění strategických záměrů firmy. Absence relevantních podkladových informací logicky výrazně zvyšuje pravděpodobnost volby chybného strategického rozhodnutí a následně se tedy zvyšuje pravděpodobnost neúspěšného provedení zvolené strategie.“ (Smejkal a Rais, 2013) Strategické aplikace jsou orientovány na budoucnost a jejich přínos je do značné míry závislý na stanovené strategii dosažení cíle. Řadíme sem například aplikace BI či CRM systémy. Potenciální aplikace jsou taktéž poměrně rizikovou investicí, jelikož je jejich hodnota dána přínosem nových podnikatelských aktivit podniku. Může se jednat např. o různé expertní systémy nebo nástroje *Competitive Intelligence*.

2.13.8 Metoda HOS 8

Metoda HOS 8 nabízí ucelený pohled na informační systém podniku založený na hodnocení osmi následujících oblastí (Koch, 2010):

- hardware (HW) – tj. fyzické vybavení, spolehlivost, bezpečnost a použitelnost se SW,
- software (SW) – tj. programové vybavení, funkce, snadnost používání a ovládání,
- orgware (OW) – tj. pravidla pro provoz IS a doporučené pracovní postupy,
- peopleware (PW) – tj. uživatelé IS a rozvoj jejich schopností při užívání IS,
- dataware (DW) – tj. data používaná a uložená v IS, dostupnost, správa, bezpečnost,
- customers/zákazníci (CU) – tj. co má IS poskytovat; obchodní či vnitropodnikoví,
- suppliers/dodavatelé (SU) – tj. co IS vyžaduje od dodavatelů, vč. vnitropodnikových,
- management IS (MA) – tj. řízení IS ve vztahu k informační strategii.

Informační systém podniku je dle Kocha (2010) zkoumán z těchto hledisek, přičemž jsou zkoumány zejména způsoby řízení jednotlivých oblastí – proto došlo k zahrnutí oblasti managementu informačních systémů, jelikož řídící pracovníci mají značný přímý vliv na většinu ostatních zkoumaných oblastí. Metoda HOS 8 nezkoumá např. spokojenost zákazníků či dodavatelů nebo přesnost dat v IS obsažených, oblasti dodavatelů i odběratelů však nabývají na významu společně s tím, jak roste provázanost informačních systémů, resp. jejich integrace s jinými IS vč. například obchodních partnerů a zvětšuje se tak okruh subjektů využívajících IS a jeho aplikace. Sběr informací pro tuto metodu má dotazníkovou podobu. Jedná se o set 10 otázek z každé oblasti, přičemž je zde vždy pět odpovědí s výběrem vždy jedné možnosti (typicky: ano, spíše ano, částečně, spíše ne, ne). Tato nominální stupnice je posléze pro účely dalšího zpracování transformována do číselné stupnice („Ano“ = 5 , …, „Ne“ = 1), v případě negativních otázek je tomu naopak („Ano“ = 1 , …, „Ne“ = 5). Tato metoda nemůže už ze své podstaty pokrýt veškeré prvky a vazby v určitě oblasti IS, nicméně dané kontrolní otázky pomohou indikovat celkový stav dané oblasti.

Autor dále uvádí, že při následném zpracování odpovědí jsou vyloučeny otázky s maximálním a minimálním bodovým ohodnocením pro danou oblast a zbývající hodnoty poslouží jako základ pro výpočet aritmetického průměru s následným matematickým zaokrouhlením. Nominální význam výsledných hodnot (tedy stavu zkoumané oblasti) je taktéž kategorizován do pěti možností (velmi nízká úroveň, nízká úroveň, střední úroveň, vysoká úroveň, velmi vysoká úroveň). Po ohodnocení všech výše uvedených oblastí IS je možno přikročit k sestavení celkového modelu informačního systému, tj. ohodnocení stavu všech zkoumaných oblastí a následně určení souhrnného stavu. Výsledky je vhodné graficky interpretovat pomocí pavučinového diagramu skládajícího se ze soustavy čtyř os, do kterých jsou zakresleny výsledky všech osmi zkoumaných oblastí. Základním grafickým znázorněním souhrnného stavu je tedy osmiúhelník.

Metoda HOS 8 vychází dle autora z předpokladu, že celkový souhrnný stav IS je roven stavu jeho nejnižší složky, resp. oblasti. Slovní interpretace souhrnného výsledku je pak shodná s interpretací jednotlivých výsledků stavů dílčích oblastí. Aby bylo následně možné formulovat doporučení na zlepšení, je nutné zjištěný souhrnný stav porovnat s významem tohoto informačního systému pro podnik. Je přitom zásadní stanovit

charakter vyváženosti, jelikož za efektivní IS je považován takový IS, jehož všechny prvky jsou vyvážené. Za zcela vyvážený IS se v případě metody HOS 8 považuje takový IS, kde všechny oblasti vykazují stejné hodnoty stavu. Zcela vyvážený IS je v praxi velmi vzácným jevem a z tohoto důvodu je nutné o něm uvažovat spíše v teoretické rovině, jakožto o ideálním cílovém stavu. Charakter vyváženosti v této metodě pracuje s kategorizací na nevyvážené, vyvážené a zcela vyvážené. Stanovení významnosti IS je nutné zejména z toho důvodu, jelikož v praxi existují četná finanční omezení, a tedy spíše než o snahu o maximální souhrnné ohodnocení, je vhodné se snažit o vzájemnou vyváženost všech jednotlivých oblastí zkoumaných touto metodou, pochopitelně při dosahování takového souhrnného stavu IS, který odpovídá jeho významu pro daný podnik. Metoda HOS 8 rozlišuje tři stupně významu IS pro firmu: IS není pro chod firmy důležitý (tzn. nepřináší ani zvýšení produkce či zisku, ani výraznou úsporu pracnosti), IS je pro chod firmy důležitý, nicméně jeho krátkodobý výpadek výrazně neovlivní chod firmy a IS je pro chod firmy klíčově důležitý, jeho, byť krátkodobý výpadek, výrazně ovlivní chod firmy. Vztah významu IS a (doporučeného) souhrnného stavu IS je tedy značně důležitý. Pokud odpovídá důležitosti daného IS pro firmu, lze hovořit o tom, že je přiměřený. Tedy pro nízkou důležitost IS je doporučená nízká souhrnná úroveň, pro organizace s běžnou důležitostí IS střední souhrnná úroveň a analogicky, pro podniky s klíčovou důležitostí IS vysoká souhrnná úroveň IS. Na základě tohoto porovnání, resp. těchto výsledků je možno formulovat několik doporučení pro informační systém jako celek. V těchto doporučeních je přitom kalkulováno se třemi základními podnikovými strategiemi ve vztahu k IS – strategií expanze (tj. zacílením na skokové zlepšení IS), strategií stability (tj. postupné zvyšování efektivity) a strategií omezení (tj. omezovat prostředky vynakládané na IS) souhrnný stav IS buď odpovídá významu IS (v ideálním případě), nedosahuje významu IS nebo je naopak vyšší než jeho význam. Metoda HOS 8 má pochopitelně několik omezení – neslouží k detailnímu zkoumání IS, zejména na úrovni jednotlivých procesů a výsledky podléhají subjektivnímu hodnocení, resp. odpovědím na dané otázky, které jsou vzhledem k širokému záběru zkoumaných informačních systémů koncipovány jako všeobecné. (Koch, 2010)

2.13.9 Portál ZEFIS

Portál ZEFIS vychází principiálně z metody HOS 8 a slouží pro snadné posuzování efektivnosti informačních systémů podniků. Vyhodnocení probíhá prostřednictvím on-line dotazníku na webovém portálu. Tato metoda pomáhá identifikovat nedostatky IS jak z pohledu jeho efektivnosti, tak z pohledu jeho bezpečnosti. Audit informačního systému se provádí na základě vyplnění dílčích dotazníků zaměřených na firmu, vybraný systém atp. Vyplnění provádí povětšinou manažer, v jehož gesci informační systémy jsou, popř. kompetentní pracovníci, kteří dotečené systémy využívají. Vyplňuje se postupně audit firmy, audit systému, audit procesu a audit provozu. Dotazovaný volí vždy ze čtyř nabízených možností. Hlavním výstupem této analytické metody je soupis identifikovaných nedostatků (seřazený dle významnosti rizika na nízké, střední a vysoké) a řada doporučení, jak tyto nedostatky napravit, jelikož systém by měl být, pokud možno, vyrovnaný. Výsledky generované portálem ZEFIS, resp. tohoto interního auditu jsou indikativní a vychází z odpovědí respondentů, nicméně dobře poslouží jakožto podklad pro další, hlubší posouzení stavu IS podniku. Součástí výstupu je i grafické vyhodnocení pomocí pavučinových grafů, které znázorňují všechny dílčí oblasti IS z pohledu efektivnosti a bezpečnosti. ZEFIS umožňuje, v případě použití plné verze, také porovnání výsledků s ostatními firmami o stejné velikosti působících ve stejném oboru. Je tak možné získat informaci o tom, jak si podnikový IS stojí v porovnání s konkurencí a zda jsou identifikované nedostatky obvyklé či nikoliv.

Obrázek č. 18: Kategorizace oblastí hodnotícího systému ZEFIS
(Zdroj: ZEFIS)

Oblasti zkoumané metodou ZEFIS jsou:

- technika – výkonnost, spolehlivost a použitelnost,
- programy – vybavení, funkce, ovládání,

- data – dostupnost, správa, bezpečnost,
- zákazníci – uživatelské potřeby, zabezpečení,
- pracovníci – schopnosti, pravidla,
- pravidla – pravidla, směrnice, postupy,
- provoz – podpora uživatelů, kontrolling.

S využitím této metody bylo prostřednictvím portálu například zjištěno, že společnosti s méně než 10 zaměstnanci vykazují nejnižší hodnocení složek IS, a naopak podniky s více než 500 zaměstnanci vykazují nejvyšší skóre v hodnocení jednotlivých složek IS, což je pochopitelné, jelikož velké podniky mají větší možnosti při investování do kvality informačního systému. Hůře jsou také hodnocené oblasti dodavatelů a zákazníků, s výjimkou společností zaměstnávajících více než 500 lidí. Velké podniky mají obvykle propracovanější systém komunikaci s vnějším prostředím. Největší pozornost je přitom takřka vždy u všech typů podniků věnována softwaru. (Chvátalová a Koch, 2015)

3 ANALÝZA SOUČASNÉHO STAVU

Analýza současného stavu sestává z představení zkoumané společnosti vč. popisu některých specifik sociálního podniku, které je nutné brát v potaz, a provedení analýz. Nejprve budou užity analytické metody zaměřené na předmětný podnik a jeho okolí (SLEPTE, Porterův model pěti sil, Analýza 7S, Analýza stakeholderů ad.) a posléze i na zkoumaný informační systém (tj. popis informační infrastruktury podniku, McFarlanův model, metoda ZEFIS, primární empirický výzkum ad.).

3.1 Představení společnosti

Společnost sales24, s.r.o. je sociální podnik, který sídlí v Brně a působí od roku 2013 pod brandem Kolibřík CSR v oblasti outsourcingu administrativy. Firma sales24, s.r.o. spadá do skupiny sociálních firem *Skupiny Kolibřík*.

Obrázek č. 19: Loga Skupiny Kolibřík a Kolibřík CSR
(Zdroj: autor)

Sociální firma má při svém podnikání za cíl zaměstnávat občany znevýhodněné na běžném pracovním trhu (Kolibřík CSRteam, c2022). Zaměstnávání zaměstnanců na tzv. chráněném trhu práce má svá specifika a pro uznání statutu je třeba, aby splňovala řadu definovaných podmínek dle Ministerstva práce a sociálních věcí (MPSV), např. že více jak polovina zisku se pak reinvestuje a slouží k navyšování hodnoty pracovního prostředí. Pro sociální podnik je však stejně jako zvýšení veřejného prospěchu důležité i dosahování zisku, nejedná se tedy o neziskovou organizaci.

3.1.1 Historie podniku

Firma nejdříve provozovala vlastní brněnské kontaktní centrum, které pracovalo na projektech společností MND, NN ŽIVOTNÍ POJIŠŤOVNA a dalších klientů. Postupem času se agenda rozšířila primárně z projektů zákaznické péče i na backoffice a do dalších měst. S rozšířením aktivit vznikly i nové společnosti, které se zaměřují na konkrétní činnosti outsourcingu zákaznických procesů a především administrativy. Toto

kontaktní centrum na konci roku 2019 odkoupil tuzemský lídr na trhu call center, společnost Comdata, a. s., která touto akvizicí vytvořila dceřinou firmu Comdata PRO (Kosour, 2021). Tak rázem vznikl sociální podnik působící v 11 regionech České republiky. S pozdější implementací směrnice GDPR v tuzemském prostředí a z toho vyplývajících omezení pro telemarketing se toto ukázalo být strategickým krokem.

Kolibřík tedy změnil svůj business model a namísto provozování vlastního centra se rozhodl vykonávat outsourcing přímo u korporátních klientů. V návaznosti na tuto změnu došlo v roce 2021 také k rozšíření činností do více segmentů spojeném s (de iure) rozdělením aktivit společnosti do pěti právně samostatných subjektů, tak aby jejich zaměření více odpovídalo specifikům jednotlivých oborů. Tak došlo ke vzniku společností Kolibřík Dokument s.r.o., Kolibřík Services s.r.o. (zaměřené na optimalizaci podatelen a pošty) nebo například Kolibřík CSR s.r.o. (orientované na služby zákaznické péče) – tedy společností sdružených ve Skupině Kolibřík. Na této změně lze ilustrovat pokračující trend přechodu od call center směrem k administrativě – například třídění bankovních dokumentů pro ČSOB v Hradci Králové, backoffice pro ČSOB v Praze, IT testing pro společnost MONETA nebo zákaznický servis pro DPD v Brně. V případě DPD je primární náplní práce zejména péče o zákazníky – odesílatele, nikoliv však pro key account, ale zejména pro menší a střední podniky odesílající méně než 100 zásilek měsíčně.

Změna obchodního modelu se nicméně dotkla i oblasti informační bezpečnosti – obecně klesly nároky na ochranu dat, jelikož původní call centrum generovalo velké množství citlivých údajů, kromě databází navolávaných čísel i např. záznamy částí hovorů. Po změně obchodního modelu, resp. odprodeji kontaktního centra, se určitá část zodpovědnosti za informační bezpečnost částečně přesunula na jejich klienty, jelikož řadoví zaměstnanci povětšinou pracují na technice (pracovních stanicích) klienta a také se zodpovídají jeho bezpečnostní politice, která se mnohdy vyznačuje přísným přístupem a vysokým stupněm zabezpečení, jelikož se pracuje například s citlivými bankovními daty, která jsou chráněna zvláštními předpisy. Tyto vztahy jsou smluvně zakotvené včetně nejrůznějších SLA (Service-level agreement).

Ve zkratce lze však konstatovat, že společnosti se tato změna strategie vyplatila. Během posledních dvou, tří let prošla Skupina prudkým růstem, kdy se zněkolikanásobil počet jejich zaměstnanců na současných bezmála 130 (resp. cca 90 FTE, což je způsobeno tím, že se zde vyskytuje větší množství kratších úvazků) a rostl obrat i zisk. V současné době (2022) tedy firma stále působí na trhu B2B a jejími klienty jsou v drtivé většině velké korporace z bankovního sektoru, logistiky nebo pojišťovnictví.

3.1.2 Sociální podnik ve strukturách korporátu

Týmy *Kolibříků*, jak své zaměstnance vedení firmy někdy označuje, se většinou staví přímo v daných korporátních společnostech. Všechny pozice, které Kolibřík vytváří, přizpůsobuje zdravotním omezením svých zaměstnanců. Firma se však důsledně snaží vyhnout vytváření „bublin", které sdružují pouze hendikepované, resp. osoby zdravotně postižené (OZP) či osoby zdravotně znevýhodněné (OZZ). S důrazem na integraci tak vznikají fungující týmy, kde jsou *Kolibříci* součástí klasických kolektivů bez hendikepu. A ačkoliv jsou tito lidé zaměstnáni u Kolibříka, dlouhodobé integrační zkušenosti ukazují, že je jejich „zdraví" spolupracovníci vnímají jako své plnohodnotné kolegy. Jedná se tak o outsourcing části vlastních činností, kde korporátní společnosti získávají benefity v oblasti náhradního plnění a dotované pracovní síly, která je vždy levnější než jejich vlastní náborová činnost. Pro korporátní klienty je tato spolupráce výhodná – umožňuje jim rychle řešit své omezené personální kapacity, snížit mzdové náklady (prostřednictvím uplatnění náhradního plnění) a posílit marketing o prvky společensky odpovědného podnikání (CSR) tím, že pomáhá zvyšovat zaměstnanost osob do značné míry vyloučených z běžného pracovního trhu.

Zdravotně znevýhodnění zaměstnanci pak získávají důstojnou práci v bezpečí sociální firmy, která jim vytváří podmínky uzpůsobené na míru. Zaměstnancům nabízí mimo jiné vysoce flexibilní pracovní dobu (převažují zkrácené úvazky) i přizpůsobené benefity. Poměrně dost často však této snaze o integraci předchází skepse ze strany zákazníků, obavy, že například tito zaměstnanci budou nespolehliví, nedokážou se dobře integrovat, budou často nemocní apod. Reálně se též stává, že si někteří zprvu myslí, že jde o mentálně postižené pracovníky nebo že každý člověk s invalidním důchodem či statusem osoby zdravotně postižené (OZP) je automaticky vozíčkář. V poslední době lze však i v českých podmínkách vysledovat pozvolné ubývání těchto

stereotypů, což může být způsobeno i obecně vyšším tlakem na společenskou odpovědnost podniků (CSR).

Celkově z těchto přibližně 130 zaměstnanců, které Skupina Kolibřík nyní zaměstnává, tvoří, včetně manažerských pozic a vedení, přibližně 80 % zdravotně znevýhodnění zaměstnanci, přičemž zastoupeny jsou osoby ve všech třech stupních invalidity. Skupina má nyní své zaměstnance v řadě měst – především pak v Brně, Hradci Králové a Praze. Centrála společnosti, kde sídlí administrativní tým, je však stále v Brně.

3.1.3 Rozvoj Skupiny Kolibřík

Od roku 2015 je Kolibřík, resp. společnost sales24, s.r.o. členem Komory sociálních podniků a stejně jako přibližně polovina sociálních podniků v České republice také členem Asociace společenské odpovědnosti z čehož plynou další závazky nad rámec těch povinných. V současné době společnost sales24, s.r.o. stále působí na trhu B2B a jejími klienty jsou v drtivé většině velké korporace ať už z bankovního sektoru, logistiky nebo pojišťovnictví. Společnosti Skupiny Kolibřík také pravidelně umožňují (i placené) stáže pro studenty, čehož se hojně využívá zejména ve spolupráci s Provozně ekonomickou fakultou Mendelovy univerzity v Brně.

Nejnovější iniciativou Skupiny Kolibřík je společně s dalšími sociálními podniky, jako například pražským Etincelle, zvyšovat povědomí o sociálním podnikání v ČR a podílet se na připravované novele zákona o sociálním podnikání tak, aby se jasně vymezil pojem sociálního podnikání v české legislativě a odlišily se malé sociální podniky od velkých firem „přeprodávajících“ náhradní plnění. Korporátní společnosti v takových případech pak poměrně rychle narazí na limit přijatého náhradního plnění, zatímco malé a střední sociální podniky jsou na cca třetině svých možností. Tyto tzv. Kulaté stoly, na kterých probíhají diskuse zástupců podniků, politiků i odborníků, jsou pak pro větší transparentnost povětšinou živě přenášeny na internet.

3.1.4 Ekonomické výsledky podniku

Z ekonomického pohledu je nejdůležitějším zákazníkem společnost ČSOB, která se dlouhodobě podílí na výnosech společnosti téměř z poloviny, což souvisí s prohlubováním vzájemné spolupráce a rozšiřováním působnosti *Kolibříků* i na oddělení IT a Digitalizace. V současné době působí *Kolibříci* na několika odděleních,

jedná se např. o Finanční trhy, IT podporu, back-office, kontaktní centrum nebo administrativní činnosti různého druhu (např. třídění došlých reklamací, problémy s transakcemi, třídění dokumentů, přepis listin atp.). Dalším důležitým zdrojem financování je státní příspěvek (dotace) na zaměstnávání osob zdravotně postižených (OZP). Státní dotace však nejsou hlavním zdrojem příjmů podniku – výnosy z vlastní ekonomické činnosti dlouhodobě dosahují necelých 60 %. Hospodaření podniku také pomáhá, že dle současného business modelu jsou mzdové náklady přímo fakturované klientům, resp. partnerským společnostem, u nichž zaměstnanci Kolibříka svoji činnost vykonávají.

Nejvyšší podíl nákladů, pak připadá na mzdy zaměstnanců (cca 65 %), management, administrativu, automobily a pojištění. Obrat společnosti za poslední účetní období (2020, novější data nebyla k dispozici) dosáhl 32.648.000 Kč a zisk po zdanění 450.000 Kč (Kosour, 2021). Společně s překotným rozvojem společnosti a zvýšením počtu zaměstnanců začala navíc sílit potřeba efektivnějšího využívání informačního systému.

3.2 Analýzy podnikového prostředí

Níže jsou provedeny analýzy zaměřené na prozkoumání vnějšího i vnitřního prostředí působícího na podnik – jedná se konkrétně o SLEPTE analýzu, Porterův model pěti sil, Analýzu 7S, stejně jako o analýzu stakeholderů. Výsledky jsou následně sumarizovány v matici SWOT analýzy.

3.2.1 SLEPTE analýza

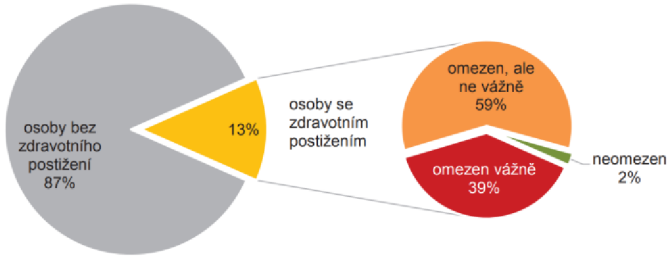
Analýza SLEPTE je účinným nástrojem ke zhodnocení vlivů vnějšího prostředí podniku, tj. externích faktorů.

3.2.1.1 Sociální faktory

Mezi významné sociální faktory, které podnik ovlivňují, lze, vzhledem k faktu, že se jedná přímo o sociální firmu, řadit podíl osob zdravotně postižených (OZP) či zdravotně znevýhodněných (OZZ) na trhu práce v České republice aktuálně hledajících práci. Tento podíl vykazuje dle Českého statistického úřadu každoročně mírně rostoucí trend. V České republice bylo v roce 2018 přibližně 13 % osob se zdravotním postižením.

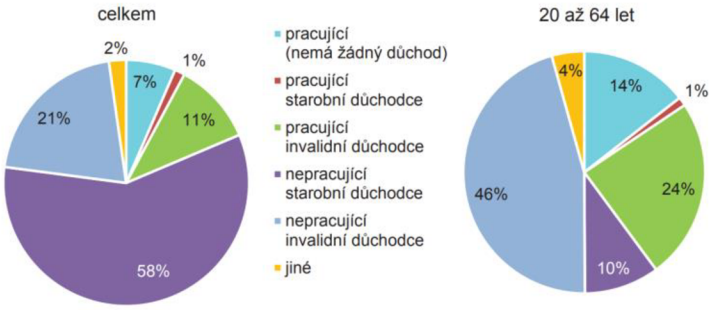
Jedná se o více než 1 150 000 dlouhodobě omezených občanů starších patnácti let. U více než poloviny z nich byl zhoršený zdravotní stav posouzen posudkovým lékařem a byl jim přiznán buď invalidní důchod (ID) nebo příspěvek na péči (nebo mobilitu), popř. získali průkaz OZP. (ČSÚ, 2019)

Podíl osob se zdravotním postižením se dle dat ČSÚ (2019) pro muže a pro ženy, kromě nejstarší skupiny nad 80 let, příliš neliší. Obecně se rychle zvyšuje s rostoucím věkem, a zatímco u nejmladších do 34 let má zdravotní postižení necelá 3 % osob a v mladším středním věku 35 až 49 let méně než 6 %, ve starším středním věku 50 až 64 se zdravotní postižení týká 16 % osob a u mladších seniorů mezi 65 a 79 lety již 26 %.



Obrázek č. 20: Osoby se zdravotním postižením dle vážnosti omezení
(Zdroj: ČSÚ, 2019)

Osoby se zdravotním postižením jsou dle dat ČSÚ (2019) značně různorodou skupinou a jejich potřeby a potíže se značně liší zejména dle toho, v jaké oblasti se jejich zdravotní postižení projevuje. Se zdravotním postižením se část lidí už narodí, jedná se však přibližně pouze o 14 % osob se zdravotním postižením. Mnohem častějším původcem jsou různá onemocnění a to v 85 %. Úrazy si na této statistice připisují zhruba 12 %. Příčiny zdravotního postižení však někdy mohou být kombinované stejně jako onemocnění může zároveň zasahovat do vícero oblastí. U největšího počtu OZP se postižení projevuje v pohybové či tělesné oblasti.



Obrázek č. 21: Osoby se zdravotním postižením podle práce a důchodu
(Zdroj: ČSÚ, 2019)

Z dat ČSÚ (2019) je patrné, že většina (tj. 81 %) osob se zdravotním postižením nevykonává žádnou výdělečnou činnost, což je dáno zejména jejich věkovým složením, jelikož 59 % osob s postižením jsou lidé ve starobním důchodu. Zaměříme-li se na OZP v produktivním věku (tj. 20-64 let), pak 40 % (tj. 203 000 obyvatel) je pracujících, oproti přibližně dvojnásobnému (79 %) podílu v celkové populaci. Na místech určených pro OZP nebo osoby zdravotně znevýhodněné (OZZ) pracovalo 12 % pracujících osob se zdravotním postižením. Na chráněném trhu práce pak pracovalo 8 % pracujících OZP. Většinu pracujících OZP v produktivním věku tvoří invalidní důchodci (24 %). Nepracující ID tvoří největší část této skupiny (46 %). Pracujících osob, které nepobírají žádný důchod, je přibližně 14 % ze všech lidí se zdravotním postižením mezi 20 a 64 lety věku.

Z dalších demografických trendů lze zmínit růst počtu obyvatel, zejména v souvislosti s válkou na Ukrajině (2022) a následnou migrační vlnou, což povede ke zvýšení počtu osob na trhu práce vč. OZP (**O1**). Dále je zde stále pokračující trend stárnutí obyvatelstva, stejně jako stále narůstající vliv civilizačních chorob na zdraví obyvatel, s jejichž přičiněním může docházet k nárůstu počtu osob, které se označují jako zdravotně znevýhodněné (**O2**). Je přitom nutné připomenout, že být hendikepovaný neznamená být automaticky např. vozíčkář. Pro podnik jsou v současnosti atraktivní pracovní silou i studenti vysokých škol (viz. placené stáže), nicméně v podniku nemají významnější zastoupení. V budoucnu by mohly být pro podnik zajímavé také osoby sociálně vyloučené nebo dlouhodobě nezaměstnané, vše však závisí zejména na nastavené sociální politice státu.

Za zmínku stojí také současný stav pracovního trhu, kdy je stále relativně nízká nezaměstnanost, byť od roku 2020, zejména vlivem pandemie, docházelo k mírnému růstu nezaměstnanosti a následnému poklesu (2021) téměř na předchozí úroveň (ČSÚ, 2022a). Lze však očekávat, že v blízké budoucnosti bude vlivem několika faktorů nezaměstnanost pomalu narůstat.

3.2.1.2 Legislativní faktory

Legislativní prostředí ovlivňuje sociální podniky velmi silně, jelikož sociální podnikání se v tuzemsku řídí celou řadou předpisů a zákonů, viz. například nutnost reinvestice zisku v souladu se závazkem k Ministerstvu práce a sociálních věcí (MPSV). Pro

sociální podniky je zcela esenciální získávání státního příspěvků na znevýhodněné zaměstnance, na kterých je provoz sociálních podniků závislý a jehož omezení, například vlivem státní politiky úspor v sociální oblasti by mohlo mít neblahé dopady na celý sektor **(T1)**. Další legislativně nastavenou možností je využívání tzv. náhradního plnění, což je mj. lákavý benefit pro korporátní klienty (obecně) sociálních podniků. Případné zvýšení limitů náhradního plnění by u korporátních klientů mohlo vést k většímu zájmu o využívání outsourcingu u sociálních podniků, což často brání k dosažení vyššího podílu OZP zaměstnanců. **(O3)**

Největší výzvou je v současnosti, resp. blízké budoucnosti připravovaná novela Zákona o sociálním podnikání, jejíž znění bude hrát zásadní roli pro postavení sociálních podniků v České republice a může pro ně potenciálně znamenat i příležitost otevření, či rozšíření, chráněného trhu práce o další skupiny sociálně znevýhodněných obyvatel. **(O4)** V neposlední řadě lze zmínit například nutnost vyhovět všem požadavkům vyplývajících z GDPR.

3.2.1.3 Ekonomické faktory

Mezi zásadní ekonomické faktory lze řadit vývoj ekonomiky, resp. ekonomický růst České republiky, jelikož přímo ovlivňuje většinu klientů/zákazníků (nejen) sociálních podniků. Například spediční firmy zaznamenávají v současné době boom, což přeneseně způsobuje nárůst objednávek i počtu klientů a tím i více práce pro sociální podniky, kterým část této administrativní agendy firmy outsourcují. Růst odvětví je tedy silně závislý na růstu ekonomiky – jedná se tedy víceméně o cyklické odvětví ekonomiky. (**W1**)

Je nutné si uvědomit, že v případě sociálních podniků hovoříme o dotované pracovní síle a parametry těchto státních příspěvků a subvencí jsou pochopitelně poplatné finanční situaci ve státě. V případě zvyšování státního deficitu je nutné počítat s tím, že stát může omezovat své výdaje na politiku zaměstnávání OZP. **(T1)**

Velký vliv má i stále rostoucí inflace, která nyní dosahuje rekordních hodnot. Konkrétně míra inflace vyjádřená přírůstkem indexu spotřebitelských cen ke stejnému měsíci předchozího roku činí za březen 2022 12,7 % (ČSÚ, 2022a). V budoucnu se také dá očekávat mírnější tempo růstu HDP a zvýšení nezaměstnanosti. Sociální firmy

působící v České republice také mohou poměrně jednoduše dosáhnout na zvýhodněné bezúročné úvěry, jako je např. S-podnik.

3.2.1.4 Politické faktory

Politické faktory mají v sociální otázce úzkou spojitost s legislativními faktory, jelikož v historii lze vysledovat rozdílný trend v přístupu k veřejným financím (a státní podpoře) v závislosti na vládnoucí straně či skupině stran. Značný vliv na sociální podniky v administrativě mají jednak změny v podnikatelském prostředí obecně (tj. daňová politika, politika zaměstnanosti atp.), větší však zejména opatření týkající se zaměstnávání osob zdravotně postižených či znevýhodněných.

V České republice došlo po parlamentních volbách v roce 2021 k poměrně turbulentnímu vývoji a částečnému obratu v některých politických otázkách. Ve společném programovém prohlášení vlády (2022) sice není nic přímo k oblasti sociálního podnikání mezi prioritami uvedeno, nicméně vláda se například vyslovila, že podpoří kratší pracovní úvazky vč. výhodnějšího zdanění slevou na pojistných odvodech a že celkově zvýší flexibilitu zákoníku práce. **(O5)** Tato změna by byla pro sociální podniky potenciálně výhodná, jelikož obvykle zaměstnávají OZP na kratší úvazky (např. 4 nebo 6 hodin denně).

Jak již bylo řečeno u ekonomických faktorů, zejména vlivem koronavirové pandemie, energetické krize či války na Ukrajině, tedy vlivem událostí, jež představují značný dopad na veřejné finance, bude pro současnou vládu nutné hledat úspory po relativně uvolněné rozpočtové politice předchozí vlády, což může vést k revizi sociální politiky zaměstnanosti v ČR a potenciálně i ke snížení státní podpory. **(T1)**

Velkou příležitostí (v menší míře pak hrozbou) pro sociální podniky je nově vznikající Zákon o integračním sociálním podnikání (viz. výše – pořádání Kulatých stolů) – potenciálně přinášející výhodnější podmínky pro sociální podniky, kterým by se tak otevřel trh s novými subjekty (lidé bez domova, maminky na mateřské apod.) **(O4)**. V souvislosti s déle trvající přípravou tohoto zákona je nutné zmínit lobbing zástupců sociálních podniků tak, aby výsledná podoba co nejvíce vyhovovala jejich obchodním modelům. Z tohoto důvodu se mnohé sociální podniky sdružují do různých platforem či oborových asociací.

Provoz sociálních podniků působících na chráněném trhu práce je tedy na státní politice více závislý (viz. čerpání příspěvku na zaměstnávání OZP apod.) než v případě běžných firem, tudíž podniky by se musely fungování dle nových regulí přizpůsobit. **(W2)**

Poměrně významný je i vliv Evropské unie, především možnost čerpání dotací z Evropských strukturálních a investičních fondů (ESIF), resp. Evropského sociálního fondu (ESF) – jedná se zejména o Operační program Zaměstnanost, jenž mohly podniky využívat až do konce roku 2020. Na tento fond navázal modifikovaný ESF+ na programové období 2021–2027. **(O6)**

3.2.1.5 Technologické faktory

Mezi významné technologické faktory ovlivňující (sociální) podnikání v oblasti outsourcingu administrativy lze jednoznačně zařadit digitalizaci. Rychlá inovace v odvětví technologií, digitalizace a přibývající počet uživatelů dělajících úkony online může v dlouhém horizontu vést k ústupu ručního zpracování dokumentů, a tedy i menší poptávce po administrativních pracovnících, jak je známe dnes **(T2)**. V souvislosti s technizací administrativy je důležité zmínit, že je při náboru zaměstnanců čím dál nutnější vyžadovat zvýšenou znalost techniky, kterou ne všichni často disponují.

Pandemie koronaviru probíhající od roku 2020 způsobila masivní přechod řady zaměstnanců rozličných firem na práci z domova, což často vyžadovalo mj. potřebné technické vybavení a dostupné a stabilní internetové připojení. U některých profesí byl přechod na distanční práci možný pouze z části. Tato zkušenost s větší digitalizací částečně přispěla ke zefektivnění některých vnitropodnikových procesů **(S1)** (např. častější online schůzky), mnohdy však přinesla také nezamýšlené důsledky a rizika v oblasti informační bezpečnosti.

3.2.1.6 Environmentální faktory

Outsourcing administrativy nepředstavuje zvlášť významnou zátěž pro životní prostředí a tohoto odvětví netýkají zvláštní regulatorní požadavky. Zmínit tak lze např. Zákon o odpadech, případně některé další legislativní normy vztahující se k podnikání obecně.

V posledních letech je patrný větší tlak společnosti na společenskou odpovědnost firem (CSR) a tím je i vyšší poptávka ze strany korporátních klientů sociálních podniků, kde se dnes již jedná o jakýsi standard a tím, že pro outsourcing vybírají podniky

zaměstnávající hendikepované zaměstnance, pomáhají zvyšovat i svoji vnímanou CSR **(O7)**. Obecně však, sociální podniky s těžištěm podnikání v administrativě, nejsou příliš ovlivňovány vnějšími environmentálními faktory.

3.2.2 Porterův model pěti sil

Porterův model pěti sil (či analýza pěti sil) je nejznámějším nástrojem pro analýzu konkurenčního prostředí firmy. Tato analýza si klade za cíl odvodit sílu konkurence v analyzovaném odvětví.

3.2.2.1 Současná konkurence v odvětví

Konkurence společnosti je velmi malá a víceméně lokální **(S1)**. Konkurenční sociální firmy též nabízí možnost outsourcingu administrativy, ale spíše na dálku ve svých provozovnách a v omezených oblastech činnosti. Např. digitalizace dokumentů, zadávání papírových platebních příkazů do PC atp. Takovýchto firem je v České republice přibližně 5. Největší přímý konkurent je tak dle jednatele společnosti sociální firma Ergotep, která se spolu s Kolibříkem dělí o zakázky u ČSOB – poměr je asi 85 % zakázky pro Kolibřík, 10 % pro Ergotep a 5 % pro další sociální firmu. Náklady na změnu dodavatele nejsou pro korporátní klienty v tomto odvětví příliš vysoké **(W3)**. Úspěch brandu Kolibřík tkví zejména v kvalitnějším projektovém řízení zakázky a lepších benefitech a mzdě pro zaměstnance. Vzájemná rivalita konkurentů v odvětví je také poměrně nízká **(S2)** a její snížení, společně s lepší vyjednávací pozicí vůči státu a dalším subjektům, je mj. cílem platformy Odpovědné podnikání, popř. oborových asociací, které sdružují řadu sociálních podniků (SP) napříč republikou. **(S3)**

Identita značky Kolibřík CSR je poměrně silná **(S4)**, Skupina Kolibřík má za sebou dlouholeté zkušenosti a kladné reference od renomovaných nadnárodních korporátních firem mj. i díky rozsáhlým možnostem přizpůsobení na míru **(S5)**. Významná je i hodnota vnímaná zákazníkem (důraz na společenskou odpovědnost již v názvu brandu). Určitou roli hraje také diferenciace služeb, byť v tomto odvětví není nijak značná a je spíše vnímaná.

3.2.2.2 Vyjednávací síla zákazníků

Vyjednávací pozice zákazníků, kterými jsou tedy zejména nadnárodní společnosti je velmi silná **(W4)**, náklady na změnu jsou pro ně relativně malé, avšak sociální podniky jim mohou nabídnout funkční a vyzkoušené řešení na úsporu HR nákladů (průměrně okolo 20 %), náhradní plnění a pozitivní PR, které jinde takto nezískají, zvláště za relativně krátký čas. Sociální firmy podnikající v oblasti administrativy jsou tedy silně závislé na svých (povětšinou) korporátních zákaznících. V případě Kolibříka je zde velmi silná závislost na ČSOB, jelikož se podílí na výnosech společnosti bezmála z poloviny **(T3)**. Získávání nových zákazníků je ze strany sociálních podniků limitováno zejména personálními kapacitami.

3.2.2.3 Vyjednávací síla dodavatelů

Vzhledem k faktu, že provoz společnosti působící v administrativě není nijak zvlášť závislý na dodavatelích, náklady na jejich změnu jsou nízké a řadoví zaměstnanci vykonávají svoji práci povětšinou na pracovišti vybaveném zákazníkem, tak vyjednávací síla dodavatelů je nízká. **(S6)**

3.2.2.4 Hrozba substitutů

V současné době jsou substituty „klasické“ společnosti zabývající se outsourcingem administrativy, avšak právě díky konkurenční výhodě sociálních firem (úspora HR nákladů, náhradní plnění, pozitivní PR apod.) mohou tyto společnosti koexistovat (soc. podniky mají zpravidla menší kapacitu). Hrozbou by mohla být zpětná vertikální integrace u korporátních společností, které by samy začaly sociálně podnikat např. s nově vytvořenou dceřinou společností. V praxi k tomu však z celé řady důvodů nedochází. Model spolupráce firem Skupiny Kolibřík s korporátními společnostmi je poměrně inovativní a prospěšný pro obě strany i zaměstnance podniku. Avšak trend digitalizace a s ní související automatizace může v dlouhém horizontu vést k ústupu například ručního zpracování dokumentů, a tedy i ke snížení poptávky po outsourcingu některých administrativních úkonů v podobě, jak ji známe dnes **(T2)**.

3.2.2.5 Nová konkurence v odvětví

Je třeba zdůraznit, že v rámci sociálních firem nejde o zcela klasickou konkurenci. Vlivem zapojení státní podpory se nejedná o ryze tržní prostředí a sociální firmy spolu nezřídka kdy také kooperují **(S7)**, přičemž jejich společný cíl je zaměstnávat více osob se zdravotním postižením. To ovšem může fungovat pouze omezeně, pokud je zde malé množství sociálních podniků působících v odlišných lokálních oblastech. Zvýšení počtu sociálních podniků nebo jejich lokální kumulace v oblastech např. administrativy, by mohlo být konkurenční hrozbou **(T4)**.

Ačkoliv tu nejsou žádné specifické bariéry vstupu do odvětví, pro naplnění definice sociálního podniku (resp. sociálního podnikání) je třeba splňovat řadu podmínek MPSV. Jedná se zejména o principy sociální, ekonomické (např. reinvestice většiny zisku) i environmentální.

Pro nové konkurenty může být bez referencí a předchozích zkušeností se sociálním podnikáním obtížné získat zájem korporátních klientů **(S8)**, jelikož ti jsou, i v současné době, ke spolupráci se sociálními firmami mnohdy zdrženliví a zejména ze strany jednotlivých manažerů bohužel často plynou obavy o vycházení s hendikepovanými zaměstnanci na pracovišti.

Pokud by došlo, vlivem schválení nového Zákona o integračním sociálním podnikání, k rozšíření sociálně znevýhodněných skupin na další skupiny obyvatel, je možné očekávat, že by to v delším horizontu vedlo ke vstupu dalších podnikatelských subjektů do odvětví. Naopak přísnější státní regulace v oblasti sociálního podnikání by mohla podnikatele od této formy podnikání odradit.

3.2.3 Analýza 7S

Analýza 7S patří mezi analýzy interních faktorů a zahrnuje množinu sedmi základních faktorů („tvrdých“ i „měkkých“), které se vzájemně ovlivňují.

3.2.3.1 Strategie

Společnost sales24, s.r.o., resp. celá Skupina Kolibřík působí na B2B trhu a jejími zákazníky jsou z drtivé většiny velké nadnárodní korporátní společnosti. Podnik svým klientům nabízí individuální řešení na míru, tedy každá zakázka či projekt jsou plně

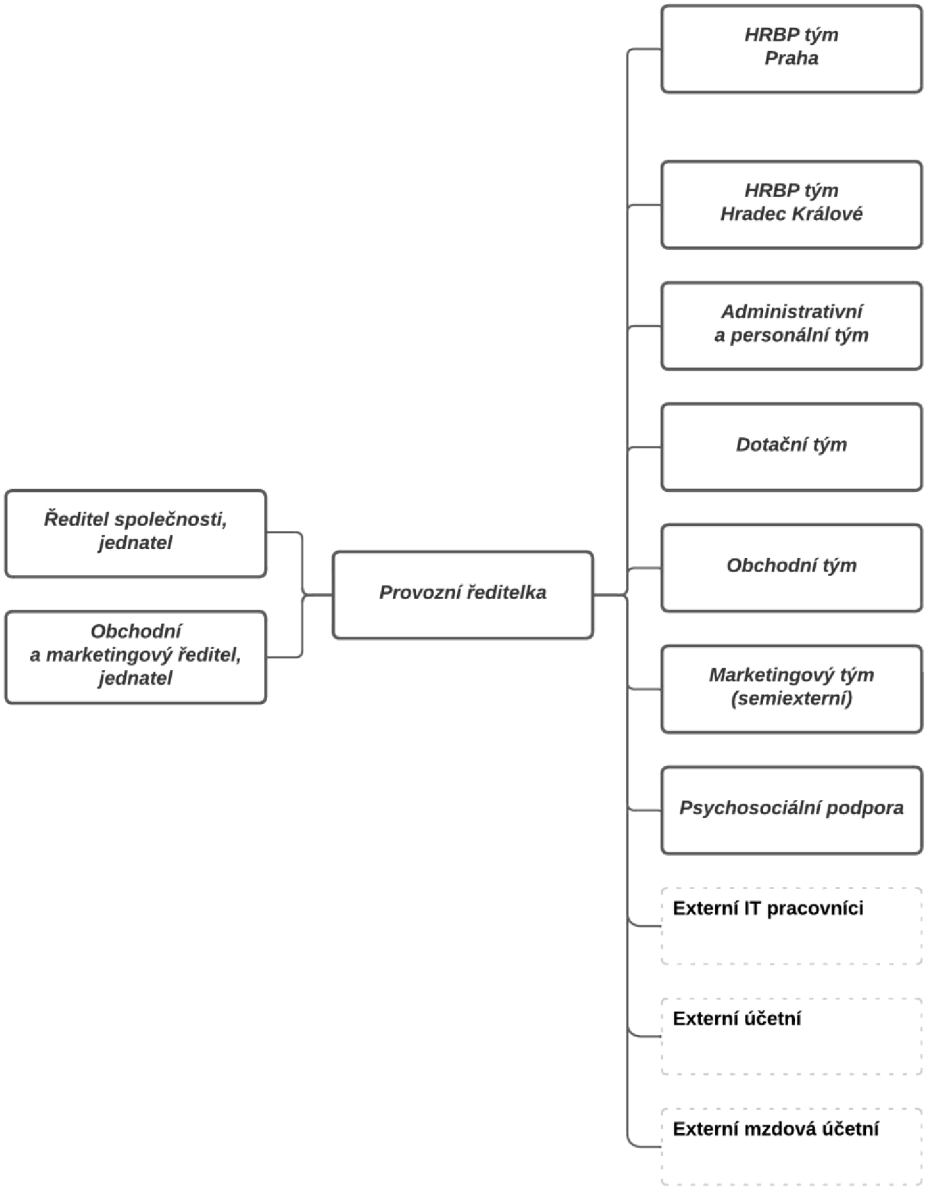
uzpůsobeny potřebám dané organizace (bankovní sektor, spediční firmy, pojišťovny, …). Vzhledem k ryze individuálnímu řešení jsou služby společnosti nabízeny po celé České republice, avšak hlavními centry zájmu je Praha, Hradec Králové a Brno.

Firma si velmi zakládá na vysoké kvalitě poskytovaných služeb, k čemuž využívá dlouholeté know-how v oboru administrativních a zákaznických center i sociálních firem. Korporátním klientům tak nabízí bezkonkurečně levnější HR kapacity (v průměru o cca 20 %), nulové náborové náklady a v neposlední řadě pozitivní PR v podobě důrazu na společenskou odpovědnost, která je v prostředí velkých společností stále aktuálnějším tématem. Zdravotně postiženým zaměstnancům tato spolupráce přináší stabilní a důstojnou práci na míru (mnohdy např. ergonomicky přizpůsobené pracoviště), povětšinou na zkrácený úvazek s ohledem na jejich možnosti a schopnosti. Stát zase poměrně efektivně řeší problematiku osob znevýhodněných na trhu práce (potenciálně tak může například ušetřit na sociálních dávkách). Jedná se tak víceméně o všestranně výhodný business model. **(S9)**

3.2.3.2 Organizační struktura

Organizační struktura společnosti naplňuje znaky funkcionální organizační struktury (zejména u administrativního týmu na centrále, popř. u externích pracovníků), avšak ve vztahu k řadovým pracovníkům se jedná spíše o klasickou organizační strukturu liniovou. Při posuzování celku lze tedy hovořit o hybridní organizační struktuře. Vzhledem k počtu manažerů je organizační struktura poměrně plochá a relativně centralizovaná. Je důležité zmínit, že se centrum organizace nachází v Brně, kde sídlí administrativní zázemí celé skupiny. Z Brna jsou tudíž řízena i pracoviště v Praze (2x) a zejména Hradci Králové, kde má Kolibřík na dvou pracovištích (ČSOB a Třídírna dokumentů) nejvíce svých zaměstnanců.

Vedení společnosti je tvořeno dvěma jednateli firmy (ředitel společnosti, obchodní a marketingový ředitel) a provozní ředitelkou. Následuje několik týmů – např. marketingový, dotační nebo obchodní a pak jsou zde dva týmy (dle lokace) tzv. HR business partnerů (HRBP) pečujících o řadové zaměstnance. Každý HRBP má na starost cca 15-25 řadových zaměstnanců. Jak je z organigramu patrné, role a odpovědnosti se mnohdy vzájemně prolínají, nelze tedy rezolutně říci, že například obchodní a marketingový ředitel by měl v gesci pouze obchodní a marketingové týmy.



Obrázek č. 22: Organizační diagram podniku
(Zdroj: autor)

Dále v podniku působí například externí účetní, externí mzdová účetní, HR náborář, PR specialistka, externí marketingoví pracovníci (sociální sítě, weby apod.), externí IT pracovníci a dotační tým, který má na starost zpracování žádostí o příspěvek na podporu zaměstnávání OZP.

3.2.3.3 Systémy

Vzhledem k velmi rychlému růstu firmy, kdy se ze společnosti o cca 30 zaměstnancích stala během bezmála dvou let společnost o více jak 100 pracovnících, je řada procesů, postupů a směrnic neukotvena, či písemně ukotvena pouze neformálně **(W5)**. Jiná je však situace zaměstnanců pracujících v bankovním sektoru, kteří podstupují pravidelná školení a certifikace potřebné pro výkon své činnosti. Tito zaměstnanci také při výkonu své činnosti pracují se zcela odlišným okruhem systémů vztahujících se k zákazníkovi, u kterého tuto činnost vykonávají. Požadavky na tyto systémy kladené, jejich kvalita i hledisko bezpečnosti, to vše je v tomto případě velmi různorodé a liší se napříč jednotlivými korporátními klienty. V poslední době došlo k zavedení *Document Management* systému (DMS), který významnou měrou usnadnil oběh dokumentů mezi jednotlivými pracovišti a víceméně již odpovídá požadavkům kladeným na bezpečnost.

3.2.3.4 Styl řízení

Styl řízení je konzultativní. Jedná se o oboustrannou komunikaci mezi manažery a podřízenými pracovníky, kdy se očekává intenzivní zpětná vazba a rozhodnutí je učiněno až po řádné konzultaci. Každý tým pracovníků má k dispozici tzv. HR Business Partnera, který funguje jako prostředník mezi ním a nadřízeným pracovníkem v dané společnosti pro kterou je outsourcing vykonáván.

3.2.3.5 Spolupracovníci

Společnost zejména díky dlouholeté praxi se zaměstnáváním OZP vyniká tím, že umožňuje velmi flexibilní plánování směn a přizpůsobení se požadavkům zaměstnanců s nejrůznějším typem hendikepů. Firma také nabízí rozsáhlý systém benefitů a soustředí se na osobní rozvoj svých zaměstnanců. Nově ve firmě působí také full-time sociální pracovnice se specializací na vzdělávání dospělých, která mj. pomáhá řešit specifické potřeby zaměstnanců.

Typické požadavky na kvalifikaci zaměstnanců nelze paušálně shrnout – firma nabízí celou řadu pozic – od běžné administrativy a např. třídění bankovních dokumentů, kde je vyžadována maturita až po odborné činnosti specialistů na finančních trzích, kde je nutné vysokoškolské vzdělání a nejlépe praxe v oboru. Určitým specifikem sociálních podniků je složitější nábor a integrace nových pracovníků **(W6)**. Fluktuace

zaměstnanců, se kterou se firma potýkala zvláště v době, kdy provozovala vlastní call centrum, je dnes už relativně nízká, avšak nábor nových zaměstnanců je stále pochopitelně velice důležitou součástí chodu firmy.

3.2.3.6 Sdílené hodnoty

Kultura úspěšné organizace musí být postavená na hodnotách, které jsou pro všechny zaměstnance známé a jsou s nimi ztotožněni. Tyto hodnoty by měly žádoucím způsobem usměrňovat jejich chování a takovéto hodnoty jsou nastaveny i v této firmě. Kolibřík se snaží budovat silnou firemní kulturu se kterou se zaměstnanci mohou ztotožnit. Jelikož má více jak cca 80 % *Kolibříků*, vč. managementu, nějakou formu hendikepu, je právě i toto jeden z atributů, který je spojuje. Kolibřík se snaží vytvářet přátelské prostředí, které umožňuje se znevýhodněným zaměstnancům plnohodnotně zapojit a přináší jim tak důstojnou a smysluplnou práci právě zejména díky, od běžných firem odlišenému, přístupu. Odtud pochází i název Kolibřík Kolibříci jsou endemičtí živočichové, kteří mají v ptačí říši neuvěřitelné schopnosti (drží řadu rekordů), avšak potřebují speciální podmínky příznivé k jejich výskytu.

Společnost je také dlouholetým aktivním členem Asociace společenské odpovědnosti a svůj provoz zakládá na principech udržitelnosti a společensky odpovědného podnikání. Firma také v loňském roce zřídila Colibri Fond a v rámci zkvalitnění pracovního prostředí se také začala pravidelně a podrobně zjišťovat spokojenost všech zaměstnanců na všech pobočkách.

3.2.3.7 Schopnosti

V Kolibříku se schopnosti a dovednosti zlepšují prostřednictvím různých školení, například školení pro manažery. Neméně důležité je však i školení zaměstnanců pro každého klienta zvlášť dle jeho potřeby. Je nutné zmínit, že požadavky kladené na zaměstnance se výrazně liší dle pracoviště (backoffice, zákaznické centrum, IT tester apod.), jelikož jsou zaměstnanci rozprostřeni mezi klienty firmy. Kolibřík začal v poslední době klást větší důraz na rozvoj zaměstnanců, což souvisí i se zřízením nové pozice lektorky specializující se na vzdělávání dospělých. Ve firmě je snaha o kontinuální rozvoj zaměstnanců a poměrně nově je jim k dispozici i stálá psychosociální pomoc.

3.2.4 Analýza stakeholderů

Níže je provedena základní analýza zainteresovaných stran a jejich zájmů na stupnici odhadovaného vlivu (0 – žádný vliv, +5 – střední vliv, +10 – maximální vliv a vice versa).

Tabulka č. 1: Analýza stakeholderů
(Zdroj: autor)

Stakeholder	Očekávání	Cíle	Síla	Vliv na podnik
Věřitelé	Splacení úvěrů	Růst zisku	Finanční prostředky	-6
Konkurence	Oslabení konkurence	Zisk většího tržního podílu	Velikost podniků, reference	-3
Lidé žijící v okolí	Zaměstnanost	Snížení nezaměstnanosti	Zájem/nezájem o pracovní pozice	+3
Zaměstnanci	Zvýšení mezd, odměny a benefity	Udržení pracovního místa, příjemné pracovní prostředí	Zvyšování produktivity společnosti	+5
Zákazníci	Snížení ceny, zvýšení kvality	Kvalitní a levná pracovní síla, posílení CSR	Odchod ke konkurenci	+8
Stát	Zaměstnávání OZP a OZZ	Integrace OZP	Legislativa vztahující se k soc. podnikání, nastavení daňové politiky	+9
Vlastníci & management	Rozvoj podniku, maximalizace zisku	Růst zisku, poboček, tržní síly, zvýšení počtu zaměstnanců	Knowhow	+10

3.2.5 SWOT analýza

Provedená SWOT analýza slouží k sumarizaci výše uvedených analýz do podobny silných a slabých stránek podniku a příležitostí a hrozeb. Pořadí je sestaveno dle uvedení v textu výše.

3.2.5.1 Strengths (Silné stránky)

- Velmi malá a víceméně lokální konkurence. (S1)
- Nízká vzájemná rivalita konkurentů. (S2)
- Lobbing platforem a oborových organizací při přípravě novely zákona o SP. (S3)
- Silná identita značky Kolibřík CSR. (S4)
- Dlouholeté zkušenosti a kladné reference od renomovaných nadnárodních korporátních firem mj. díky možnostem přizpůsobení na míru. (S5)

- Nízká vyjednávací síla dodavatelů. (S6)
- Podnik nepůsobí na ryze konkurenčním trhu vlivem velkého zapojení státní podpory. (S7)
- Zhoršený vstup do odvětví pro nové konkurenty vlivem absence referencí (zdrženlivost korporátních zákazníků). (S8)
- Všestranně výhodný business model. (S9)

3.2.5.2 Weaknesses (Slabé stránky)

- Silná závislost společnosti i odvětví na růstu ekonomiky. (W1)
- Vysoká závislost na státní politice v oblasti zaměstnávání OZP. (W2)
- Nízké náklady na změnu dodavatele v případě zákazníků. (W3)
- Velmi silná vyjednávací pozice zákazníků (zvl. nadnárodních korporací). (W4)
- Neukotvenost a neformálnost řady procesů, postupů a směrnic vlivem překotného růstu společnosti. (W5)
- Složitější nábor a integrace nových pracovníků. (W6)

3.2.5.3 Opportunities (Příležitosti)

- Růst počtu obyvatel vč. OZP, zejména v souvislosti s válkou na Ukrajině (2022), resp. následnou migrační vlnou. (O1)
- Trend stárnutí obyvatelstva, stejně jako stále narůstající vliv civilizačních chorob na zdraví obyvatel, s jejichž přičiněním může docházet k nárůstu počtu osob, které se označují jako zdravotně znevýhodněné. (O2)
- Případné snížení limitů náhradního plnění by u korporátních klientů mohlo vést k většímu zájmu o využívání outsourcingu u (zvláště menších) sociálních podniků generujících vysokou přidanou hodnotu, což nyní často brání k dosažení vyššího podílu OZP zaměstnanců. (O3)
- Připravovaná novela Zákona o sociálním podnikání, jejíž znění bude hrát zásadní roli pro postavení sociálních podniků v České republice může znamenat i příležitost otevření, či rozšíření, chráněného trhu práce o další skupiny sociálně znevýhodněných obyvatel. (O4)
- Vláda ČR se v programovém prohlášení vyslovila, že podpoří kratší pracovní úvazky vč. výhodnějšího zdanění slevou na pojistných odvodech a že celkově zvýší flexibilitu zákoníku práce. (O5)

- Možnost čerpání dotací z Evropských strukturálních a investičních fondů (ESIF), resp. ESF+. (O6)
- Tlak okolí na společenskou odpovědnost firem (CSR), což způsobuje mj. vyšší poptávku ze strany korporátních klientů sociálních podniků. (O7)

3.2.5.4 Threats (Hrozby)

- Omezení státních příspěvků a obecně výdajů na zaměstnávání OZP, vlivem hledání úspor ve státním rozpočtu. (T1)
- Trend digitalizace může v dlouhém horizontu vést k ústupu ručního zpracování dokumentů, a tedy i ke snížení poptávky po outsourcingu některých administrativních úkonů v podobě, jak ji známe dnes. (T2)
- Velmi silná závislost na ČSOB, podílející se na výnosech společnosti bezmála z poloviny. (T3)
- Zvýšení počtu sociálních podniků nebo jejich lokální kumulace v oblastech administrativy, by mohlo být značnou konkurenční hrozbou. (T4)

3.2.6 Souhrn podnikových analýz

Z analýzy SLEPTE, tj. vnějšího okolí podniku, vyplynulo, že tuzemské sociální firmy podnikající v oblasti outsourcingu administrativy z externích faktorů nejzásadněji ovlivňují zejména ty legislativně-politické a ekonomické faktory. Konkrétně má na tento sektor značný vliv stát a jeho nastavení sociální politiky. V neposlední řadě je významným externím faktorem také situace na trhu, a tudíž potřeba externího outsourcingu administrativy zejména ze strany korporátních klientů (tudíž nízká obranyschopnost vůči recesi). Velký vliv státu je znázorněn i v analýze stakeholderů.

Porterův model nám ilustruje, že se podnik nachází v poměrně atypické situaci, jelikož sociální firmy nejsou ryze tržními subjekty a byť se jedná o obchodní společnosti, a ne neziskové organizace, není zde přítomna klasická konkurence ve standardním pojetí a rozsahu. Konkurence spol. sales24, s.r.o. je poměrně malá, a navíc ještě velice lokální.

Vlivem velmi malé konkurence (S2), nízké míry rivality (S3) a dlouholetých zkušeností (S5) by v případě snížení limitů náhradního plnění (O3), popř. rozšířením chráněného trhu práce i na další skupiny obyvatel (O4) či díky větší podpoře kratších flexibilnějších úvazků ze strany vlády (O5) může docházet k navýšení počtu zakázek, stejně jako

přibývající počet OZP v populaci (O1, O2) může vést k většímu počtu zaměstnanců, bez nichž není možné dodatečné zakázky realizovat.

Případné snížení limitů náhradního plnění (O3) by u korporátních zákazníků mohlo vést k větší poptávce po využívání outsourcingu části svých činností u menších sociálních podniků, což by v delším horizontu mohlo potenciálně znamenat oslabení současné velmi silné vyjednávací pozice těchto korporací (W4). Některé kroky státu, jako např. připravovaná novela zákona o sociálním podnikání (O4), stejně jako proklamovaná vládní podpora kratších pracovních úvazků (O5) by mohly pomoci překonat složitější nábor a integraci nových pracovníků (W6). Lobbing platforem a oborových organizací při přípravě novely zákona o sociálním podnikání by mohl odvrátit potenciální ohrožení v podobě omezení státních příspěvků na zaměstnávání zdravotně postižených osob (T1).

Podnik má poměrně dobrou pozici na trhu, Kolibřík CSR je mezi sociálními podniky operujícími v administrativě relativně silný brand a proponovaný obchodní model je v současné době dobře fungující. Strategie společnosti je poměrně jasně definovaná a stejně jako mise a vize je dobře komunikovaná, což platí jak pro zaměstnance, tak i veřejnost. Má na tom značný podíl i silná osoba zakladatele, který nyní společně s dalšími dvěma řediteli řídí podnik dodnes.

Společnost prosperuje a prochází mohutnou expanzí, která se projevuje nejen na skokovém zvýšení obratu, ale i na počtu zaměstnanců. V současné době se však společnost potýká také s některými nedostatky – např. z poněkud chaotické organizační struktury i vlivem neformálních procesů plynou problémy v operativě. Na některých pobočkách je také pociťován personální nedostatek, což může potenciálně ohrožovat plnění zakázek. Je zde však přítomna snaha získat další skupiny klientů a pokračovat v expanzi, jednak do dalších oddělení stávajících klientů, ale také do dalších organizací, resp. dalších měst. Firma by ráda navázala spolupráci s dalšími subjekty, zejména z řady korporátních klientů, zvláště pak takových, kteří nesplňují stanovené minimální povinné limity na zaměstnávání osob zdravotně postižených. Podnik má pro tento další rozvoj přístup k adekvátním finančním zdrojům. Společnost musí také včas zareagovat na měnící se potřeby trhu plynoucí z digitalizace administrativy.

3.3 Analýza informačního systému

Úlohou analýz informačního systému je zmapování současného stavu podnikového IS vč. jeho efektivnosti a bezpečnosti. Pro účely této práce bude využit také mj. aplikační pohled na informační systém.

3.3.1 Informační infrastruktura

Při základní analýze podnikové informační architektury je možné vycházet např. z práce Vebera a Srpové (2012), kteří rozlišují pět elementárních komponent, jako je:

- hardware
- základní software
- peopleware
- orgware

Tuto kategorizaci je možné ještě rozšířit o pojem dataware (Molnár, 2001). Případně je možné využít rozšířenou kategorizaci informační infrastruktury užívanou v metodě HOS 8 , která nahlíží na informační systém organizací z osmi klíčových oblastí, kterými jsou (Koch, 2010):

- hardware
- software
- orgware
- peopleware
- dataware
- zákazníci
- dodavatelé
- management IS

Vzhledem k zaměření firmy a oblasti, kde podnik působí nedochází k předávání dat prostřednictvím informačního systému ani dodavatelům, ani zákazníkům, jak je to typické například pro obchodní firmy a zákazníci IS jsou tudíž pouze vnitropodnikoví. Pro účely této práce je pět základních oblastí vymezených Molnárem či Veberem a Srpovou rozšířeno ještě o významnou oblast managementu IS.

3.3.1.1 Hardware

Společnost nyní provozuje přibližně 16 notebooků – převážně se jedná o repasovaná zařízení různých značek (spol. však dle slov jednatele preferuje zn. HP), 5 stolních PC a 5 tiskáren (z nichž 3 síťové) od různých dodavatelů plus různá periferní zařízení. Podotýkám, že tato práce se nezabývá posuzováním stavu informačního systému v celé Skupině Kolibřík a nezahrnuje tudíž zaměstnance pracující na zařízeních a v IS korporátních klientů, jelikož jejich úroveň je značně odlišná. Několik kusů notebooků bylo pořízeno v uplynulém roce jednak vlivem částečného přechodu na práci z domova, ale také vlivem toho, jak v podniku roste počet zaměstnanců. Dále pracovníci společnosti používají okolo 20 mobilních telefonů různých značek a poměrně nově přibylo jedno sdílené datové úložiště (NAS) značky Synology (řady DS). Podnikovou síť tvoří různé síťové prvky, např. routery zn. TP-LINK. Kancelář je vybavena standardně zabezpečeným Wi-Fi AP, síť však není rozdělena na veřejnou a privátní část. Některá síťová zařízení jsou zabezpečena pouze výchozími hesly. Jednotlivé prvky síťové infrastruktury jsou propojeny strukturovanou kabeláží. Tato infrastruktura není v rámci kanceláře nijak chráněna proti neoprávněnému přístupu (např. monitoring portů ad.) – více viz. výzkum informační bezpečnosti. Průměrné stáří zařízení je cca 5 let, případné nákupy nové techniky se řeší ad hoc v případě potřeby, jinak se technika pravidelně neobměňuje.

3.3.1.2 Software

Ve společnosti je používána řada programů, jedná se zejména o aplikace Synology Drive, Giriton, Aplikaci Třídírna a v blízké budoucnosti zprovozněný CSRnet. Tyto stěžejní podnikové aplikace budou více přiblíženy v samostatných kapitolách níže. Mezi ostatní aplikace používané ve společnosti patří zejména některé komunikační nástroje pro rychlou komunikaci mezi manažery, jež nahrazují e – mailovou korespondenci. Konkrétně se jedná o vytvořené skupiny na IM WhatsApp, popř. využívání Skype nebo Jitsi. Někteří manažeři také používají například Trello, nejedná se však o majoritní trend. Typické je však samozřejmě používání kancelářských aplikací (kancelářský balík Microsoft Office, Microsoft Outlook apod.). Společnost provozuje e – mailové schránky na hostingu třetí strany.

Na všech pracovních stanicích je nainstalovaný operační systém Windows 10. V této souvislosti je nutné zdůraznit, že aktualizace OS je vždy na odpovědnosti jednotlivých uživatelů a je nutné upozornit na fakt, že zaměstnanci mají na svých pracovních počítačích plná administrátorská práva a mohou si tak na ně instalovat libovolný software, což činí počítač mnohem zranitelnější např. vůči virům či spywaru. Po pracovnících se pouze vyžaduje a při předání stvrzuje, že počítač je zabezpečen heslem a každý má na něm vytvořen svůj vlastní uživatelský účet. Uživatelské účty ani přihlašování uživatelů není nijak řízeno, ani řešeno např. pomocí LDAP.

3.3.1.3 Dataware

Nejcennější podniková informační aktiva jsou zejména personální složky všech zaměstnanců, přičemž ty obsahují obvykle citlivější údaje, než je běžné v jiných organizacích, což je dáno zejména tím, že se jedná o sociální firmu. V personálních složkách (digitálních i fyzických) jsou tak uložené některé dokumenty, jako je např. přiznání invalidního důchodu (ID) obsahující také podrobné lékařské zprávy či zdravotnickou dokumentaci například formou posudků. Druhou skupinou aktiv je pak podnikové účetnictví a doklady k němu se vztahujícímu, které jsou shromažďovány a předávány ke zpracování externí účetní. Dalším typem dat jsou provozní údaje, které jsou pro podnik důležité, nejsou však pro jeho chod nezbytně kritické – jedná se například o provozní data v Aplikaci Třídírna.

Nakládání s daty, resp. odpovědnost za data svěřená a zadávaná je v podniku definována velmi vágně, spíše neformálně a pouze v rovině ochrany osobních údajů. Plošně platná politika zálohování dat v podniku neexistuje, každý zaměstnanec však údajně odpovídá za jemu svěřené údaje. Problematika zálohování a ochrany dat bude blíže popsána v kapitolách níže u jednotlivých aplikací, resp. v oblasti informační bezpečnosti.

3.3.1.4 Orgware

V podniku neexistují žádné směrnice či normy a bezpečnostní pravidla vztahující se k IS/IT. Určitá pravidla jsou zakotvena v organizačním řádu společnosti, který též specifikuje některé politiky (např. *Clean desk policy*), avšak v praxi nejsou tato opatření kontrolována, ani dodržována. Řada dodatečných pravidel je spíše neformálního

charakteru a není jasně definována. Neexistuje ani jednotná politika hesel, vše je ponecháno na uvážení daného pracovníka. Každý zaměstnanec je však poučen, že odpovídá za jím svěřenou techniku, potažmo i za podniková data, avšak prakticky pouze při nástupu do zaměstnání nebo přebírání prvního pracovního počítače. Systematický monitoring bezpečnostních incidentů taktéž neprobíhá. Podnik navíc víceméně umožňuje používání vlastních zařízení na pracovišti (BYOD) – tj. např. soukromé notebooky či tablety, což může představovat značné bezpečností riziko. Podrobněji o této problematice viz. kapitola věnovaná informační bezpečnosti.

3.3.1.5 Peopleware

Školení zaměstnanců pro práci s informačním systémem, resp. jeho součástmi neexistují. Není také k dispozici žádná forma podpory vyjma asistence nadřízeného s možností povolání externího IT pracovníka. Tito externí IT pracovníci (v současné době 2 – jeden pro Brno a druhý pro Prahu a Hradec Králové) navíc prakticky řeší pouze hardware. Vzhledem k externí povaze jejich pracovního úvazku mají navíc značně omezené časové možnosti a zaměstnanci tak na podporu čekají někdy i více jak dva dny. V případě lehčích problémů, jejichž povaha je umožňuje vyřešit prostřednictvím telefonu nebo vzdáleného připojení je vzdálená podpora o něco flexibilnější. Zaměstnancům nejsou také k dispozici manuály a postupy pro řešení nejčastějších problémů jako jsou typicky například zapomenutá hesla apod.

3.3.1.6 Management IS

Společnost nemá zřízený post manažera informačních technologií a řízení IS/IT je tak primárně v kompetenci zakladatele a ředitele (resp. jednoho z jednatelů společnosti). Ten se také stará o běžnou údržbu (např. nákup licencí antivirových programů) a řešení snazších problémů. Jak již bylo řečeno výše, správu hardware mají primárně na starost dva externí IT pracovníci – jeden pro Brno, druhý pro Hradec Králové a Prahu. O případných investicích do IT rozhoduje přímo ředitel společnosti ve spolupráci s obchodním ředitelem. Společnost však na IS/IT vynakládá méně než přibližně 5 % svého obratu ročně.

Zásadním problémem je neexistující informační strategie podniku, což je dáno zejména tím, že donedávna podnik problematiku IS/IT příliš nemusel řešit a bral ji jen jako

podružnou nezbytnou nutnost. Doposud tedy bylo řízení IS poměrně okrajovým tématem pro management, v poslední době však jeho význam sílí, společně s překotným rozvojem společnosti, kdy se malá firma rapidně rozrostla o velký počet zaměstnanců, avšak oblast IT zůstává prakticky stejná, jako když měla firma pouze několik zaměstnanců. Management společnosti si začíná uvědomovat, že mnohdy již nedostačují ad hoc řešení a některé podnikové procesy je třeba řídit jinak. V souvislosti s rozvojem společnosti došlo také k výrazné změně organizační struktury, kdy vznikla pozice provozní ředitelky. Lze předpokládat, že některé oblasti bude nutné řídit více koncepčně a to vč. problematiky IS/IT.

3.3.2 Používané aplikace IS

Úkolem této kapitoly je představit nedůležitější podnikové aplikace významné pro chod společnosti. Většina procesů využívajících IS se v podniku týká administrativy, resp. personalistiky, čemuž odpovídá i podnikové aplikační portfolio.

3.3.2.1 Synology Drive

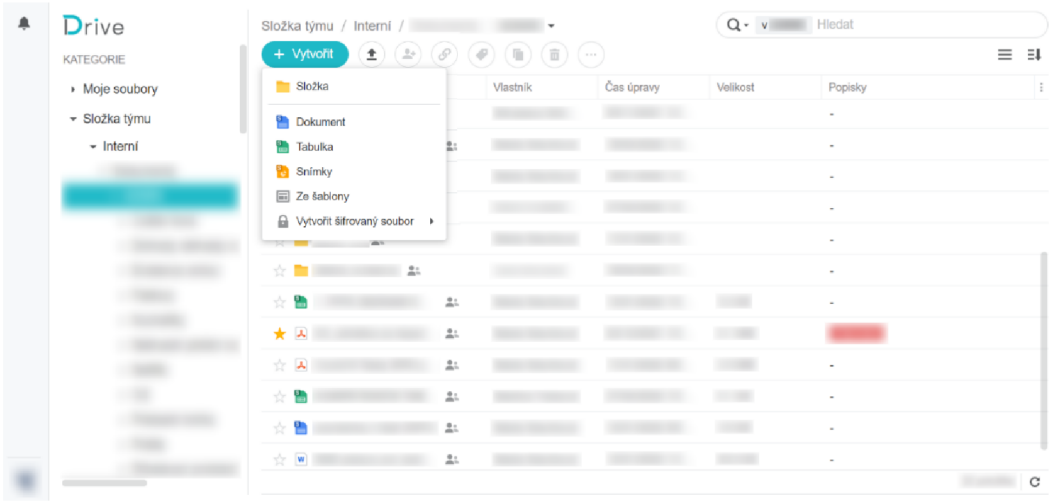
Aplikace Synology Drive patří z řady důvodů mezi zcela nejdůležitější podnikové aplikace. Synology Drive je systém sloužící ke správě a výměně dokumentů (vč. externího sdílení), jedná se tedy principiálně o DMS. Vyjma správy dokumentů umožňuje také spolupráci na dokumentech, které jsou editovatelné online. Přístup k tomuto systému je možný skrze webovou aplikaci nebo skrze lokální přístup v rámci podnikové sítě, popř. skrze mobilní aplikaci nebo desktopového klienta s názvem Synology Drive Client.

Toto řešení, tj. pořízení vlastního NAS je relativně nové – nahradilo původní řešení ve formě sdílené složky na Google Drive, k níž se manažeři přihlašovali pod jedním generickým účtem. Tato praxe byla nevyhovující z celé řady hledisek, zejména z pohledu informační bezpečnosti. Společnost se rozhodovala nad výběrem z několika možností, a nakonec dala přednost před cloudovým řešením Microsoftu relativně nízkým provozním nákladům a větší kontrole nad podnikovými daty. Implementace tohoto řešení proběhla nárazově, přičemž se vyskytlo relativně minimum komplikací. Nejvýraznější změnou oproti předchozímu řešení byla možnost nastavovat odlišná oprávnění pro různé uživatele či skupiny uživatelů. Není například přípustné, aby

dokumenty týkající se mezd zaměstnanců byly v systému volně dostupné všem uživatelům. V souvislosti s managementem uživatelských účtů je nutné zmínit, že v současnosti není v podniku systematicky řešeno přidávání nových účtů, ani odebírání přístupových práv v případě ukončení pracovního poměru.

Obrázek č. 23: Logo Synology Drive
(Zdroj: autor)

Synology Drive se používá každodenně, a to napříč podnikem. Sociální podniky zpracovávají velké množství dokumentů, zejména těch týkajících se personalistiky. Nově se tento systém využívá také k zálohování podnikového účetnictví. Synology, resp. DSM podporuje mj. také verzování dokumentů (systém uchovává až 20 verzí souborů, čímž lze řešit nechtěné přepisy), takže odpadají některé četné starosti při spolupráci více lidí na společných souborech, což značně ulehčí spolupráci mezi jednotlivými pobočkami. Zvlášť užitečná je funkce kolaborace, která umožňuje simultánní editaci více uživateli naráz, čehož se v podniku často využívá v případě sdílených tabulek. Výrazným nedostatkem tohoto řešení však bylo neočekávané postimplementační zjištění, že editace je možná pouze prostřednictvím webového prohlížeče, resp. jejich nativní aplikace Synology Office a simultánní editace např. v MS Word není v reálném čase možná, byť zde samozřejmě existuje kompatibilita mezi formáty kancelářských souborů Synology Office a MS Office.



Obrázek č. 24: Uživatelské rozhraní aplikace Synology Drive
(Zdroj: autor)

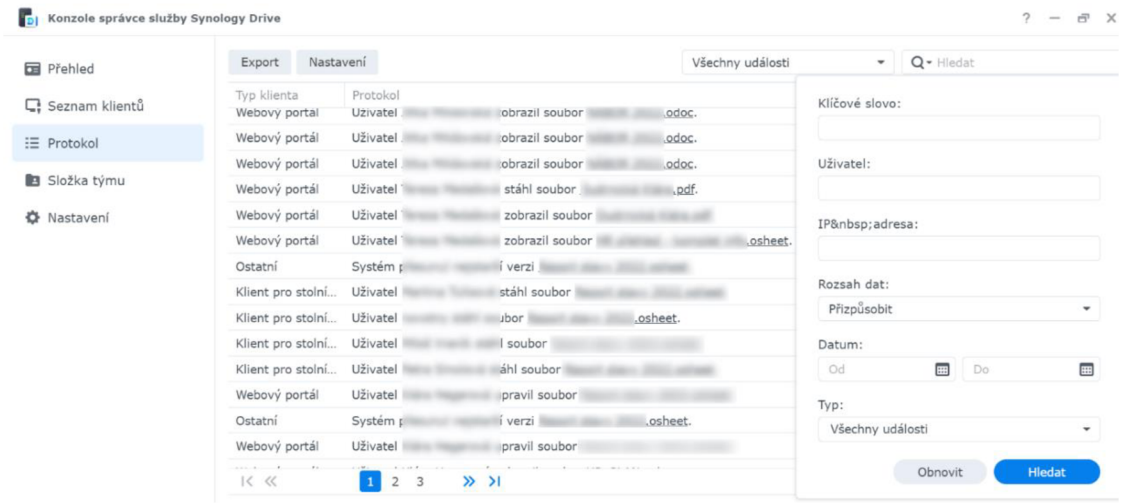
NAS Synology slouží zároveň jako privátní úložiště pro jednotlivé zaměstnance, kteří mají možnost zálohovat data se svých počítačů, byť nyní toho však v praxi příliš nevyužívají. V nastavení je možné k tomuto účelu každému uživateli alokovat určitou kvótu. Rozšířené možnosti konfigurace jsou i v oblasti přihlašování se do systému a zabezpečení obecně. Všechny administrátorské účty jsou zabezpečené dvoufázovým ověřováním.

Data používaná aplikací Synology Drive jsou uložena lokálně na NAS (*Network Attached Storage*) umístěném v brněnské centrále společnosti. Tato data jsou v pravidelných intervalech zálohována na cloud, konkrétně na Synology C2 Storage a to na denní bázi. Ochrana dat je řešena také zrcadlením (mirroring) pevných disků (tj. RAID 1). Úložiště však nemá zálohované napájení (UPS), takže v případě výpadku či odstávky elektřiny nebude mít společnost přístup k souborům. Toto lze vyřešit několika způsoby, jedním z nabízených řešení by bylo využití dalšího NAS ve fyzicky oddělené lokalitě (např. pražské pobočce) a použití řešení Synology Hybrid Share, což by mj. potenciálně zrychlilo odezvu systému při přístupu z jiných lokalit. Popřípadě je možné připojit skrze druhé rozhraní LAN (tento model NAS je vybaven dvěma porty) záložní 4G/5G modem taktéž zálohovaný UPS.

Systém DSM (DiskStation Manager) slouží ke kompletní správě NAS a obsahuje vyjma širokých možností konfigurace i pokročilé nástroje pro monitoring přístupů i využití (Active Insight) – např. uchovávání logů a generování protokolů. Skrze administrátorské rozhraní je možné řídit uživatelské účty, resp. skupiny účtů., řídit přístup k jednotlivým složkám apod. Možnosti tohoto systému jsou značné, byť je nutné dodat, že v současné době podnik nevyužívá zdaleka všechny možnosti nabízené tímto systémem.

Obrázek č. 25: Úvodní plocha administrátorského rozhraní systému DSM
(Zdroj: autor)

Aplikace Synology Drive je v současnosti aktivně používána manažery na prakticky všech stupních řízení. Někteří uživatelé přistupují z webového prohlížeče, jiní využívají lokální přístup (na brněnské centrále), někteří preferují použití klienta Synology Drive Client (celkem 11), naopak minimum uživatelů (cca 4) používá mobilní aplikaci Synology Drive, která je dostupná jak pro OS Android, tak iOS.



Obrázek č. 26: Ukázka protokolu v konzoli správce Synology Drive
(Zdroj: autor)

V současné době obsahuje aplikace 31 uživatelů a 4 uživatelské skupiny – administrátoři, OVH, uživatelé a návštěvníci. Poslední jmenovaná skupina jsou neregistrovaní externí uživatelé, se kterými je možné za určitých podmínek sdílet soubory prostřednictvím tzv. veřejných odkazů zabezpečených hesly.

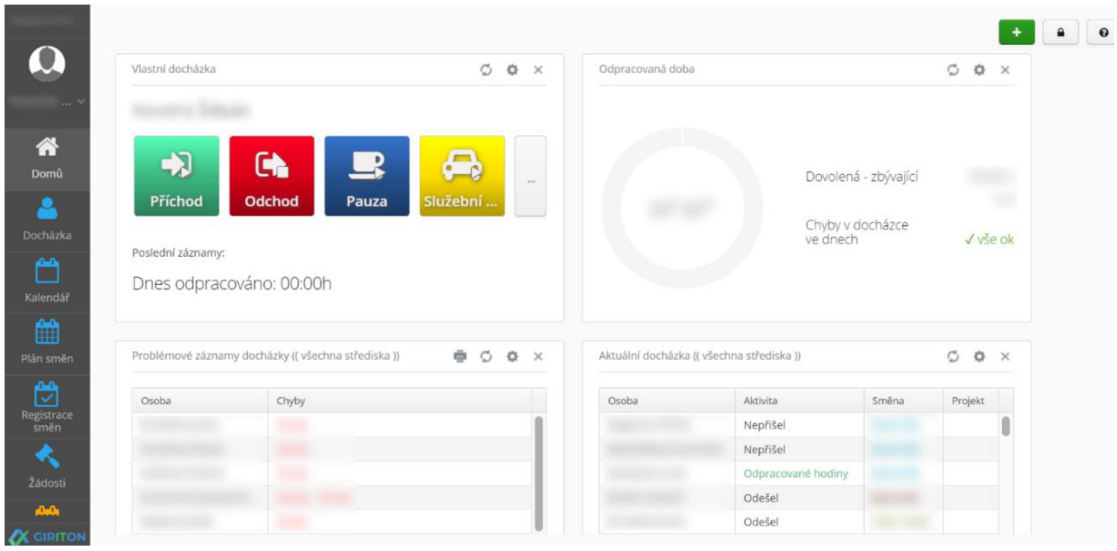
Případná delší nefunkčnost této aplikace (v řádu desítek hodin) by znamenala vážný zásah do chodu podniku, jelikož výměna informací mezi pobočkami probíhá velmi aktivně a v poměrně velkém objemu.

3.3.2.2 Giriton

Společnost také relativně nově, v zimě 2021/2022 zavedla docházkový systém Giriton, čímž nahradila dosavadní systém hlášení a následného ručního zapisování docházek do tabulkových procesorů. Giriton je software vyvinutý brněnským startupem vedeným absolventem Fakulty podnikatelské VUT Janem Gřešem, který zprvu vymyslel systém na řízení výrobních firem, jehož jednou z řady funkcí byla právě elektronická docházka. Tento docházkový modul se však brzy stal natolik žádanou aplikací, že se rozhodli zaměřit veškerou pozornost a vývoj pouze tímto směrem – tj. na docházkový systém pro všechny podniky, nejen ty výrobního zaměření. (Zprávy z VUT, 2017).

Obrázek č. 27: Logo Giriton
(Zdroj: Giriton, c2021)

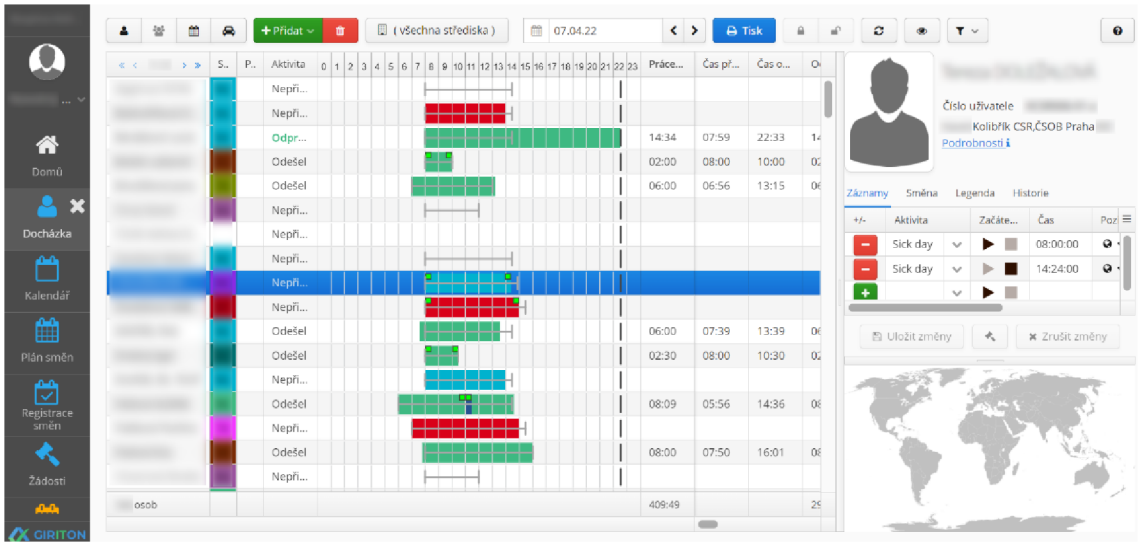
Hlavním cílem tohoto systému je dle jeho zakladatele „*usnadnit zaměstnavatelům evidenci a vykazování věcí, které mají nařízeny zákonem. Navíc tím lze zefektivnit procesy jako žádosti o dovolenou, vykazování cest a podobně, které jsou mnohdy ve firmách zbytečně složité*“ (Zprávy z VUT, 2017).



Obrázek č. 28: Uživatelské prostředí aplikace Giriton
(Zdroj: autor)

Aplikace Giriton je tedy komplexní docházkový systém umožňující vyjma přehledné a srozumitelné evidence přítomnosti na pracovišti také plánovat směny, což je v sociálním podniku s velkým počtem různě krátkých úvazků velice důležité, nebo žádat o dovolenou. V takovém případě pak nadřízenému přijde notifikace např. e – mailem s výzvou ke schválení. Funkcionalita tohoto systému je skutečně široká, nabízí také další možnosti, jako je např. plánovač projektů, převádění přesčasů, evidence příplatků, hlídání fondu sickdays, hlídání fondu dovolených, vykazování služebních cest, sdílený kalendář apod. Giriton také nabízí integraci aplikace s nabízenými píchacími hodinami (vč. například užití biometriky), tohoto řešení však předmětná společnost v současnosti nevyužívá.

V aplikaci nyní existuje několik úrovní uživatelských oprávnění – administrátorská, administrativní tým Brno, týmy jednotlivých HRBP, náhledové účty pro manažery zákazníků a především – zaměstnanci s možností zadávání vlastní docházky – těch je v současnosti přibližně polovina. Velkou výhodou aplikace Giriton je možnost uživatelů zadávat si svoji docházku i prostřednictvím mobilní aplikace. Této možnosti, resp. mobilní aplikace využívá v současnosti přibližně 40 % uživatelů.



Obrázek č. 29: Administrátorské rozhraní aplikace Giriton
(Zdroj: autor)

Jedná se o software poskytovaný jako službu (SaaS), zálohování na lokální úložiště na pravidelné bázi neprobíhá. V současné době jsou měsíční náklady na tuto aplikaci okolo 3000 Kč (bez DPH). Drobným nedostatkem, na který si někdy personalisté stěžují, je pomalejší načítání některých seznamů a generovaných tabulek. Vedoucí pracovišť, resp.

středisek mají však díky tomuto systému přehled o docházce svých podřízených a snazší je také vykazování odpracovaných hodin za účelem zpracování mezd externí mzdovou účetní. V této souvislosti se aktuálně v podniku řeší export evidence docházky pro zpracování ekonomickým systémem POHODA, resp. mzdovým systémem Pamica, který je však již nějakou dobu nativně v Giritonu podporován. Tímto způsobem bude možné předávat data mezi aplikacemi mnohem efektivněji, stále se však vyžaduje ruční export dat každý měsíc.

Giriton je v současnosti pro podnik stejně významný a důležitý jako Synology Drive, jelikož jeho případná náhlá nefunkčnost by znamenala návrat k předchozímu ručnímu systému evidence docházky, který byl z několika hledisek, zejm. toho časového, zcela dlouhodobě neudržitelný.

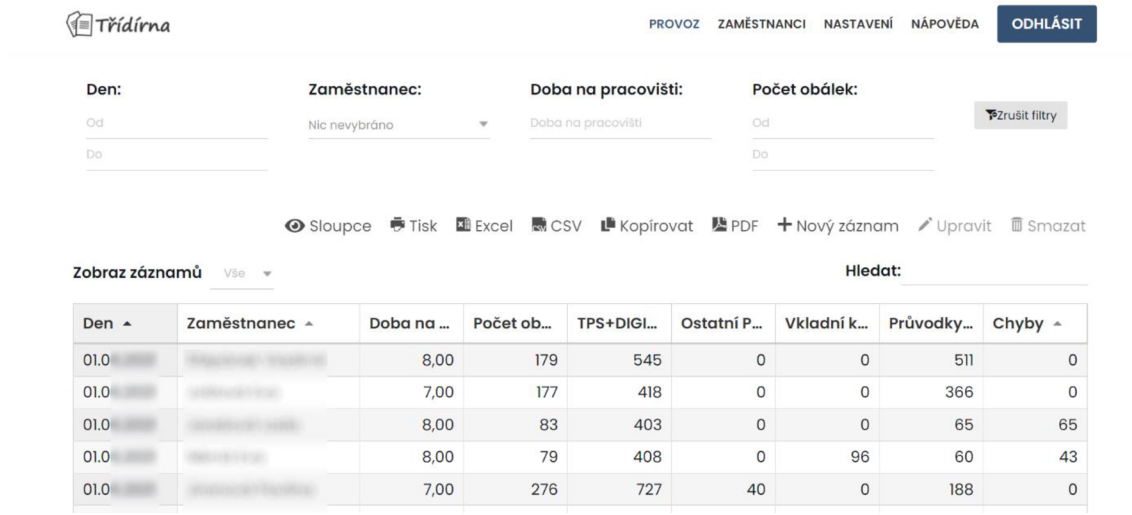
3.3.2.3 Aplikace Třídírna

Aplikace Třídírna je poměrně jednoduchá webová aplikace, resp. nástroj spadající do kategorie business intelligence (BI). Jak již název napovídá, jedná se o systém sloužící k evidenci určitých provozních údajů týkajících se pracoviště třídírny dokumentů banky ČSOB v Hradci Králové. Tato miniaplikace byla vytvořena na zakázku je určena pouze pro interní potřeby společnosti.

Obrázek č. 30: Logo Aplikace Třídírna
(Zdroj: autor)

S pomocí této aplikace se evidují provozní údaje jako například počet zpracovaných obálek, vkladních knížek, průvodek nebo počet vyřešených chyb, ale také doba na pracovišti. Před zprovozněním tohoto semiautomatizovaného řešení se údaje evidovaly ručně, načež se s měsíční frekvencí přepisovaly, pro základní analytické potřeby, do MS Excel. Tyto údaje se evidují na denní bázi, a to za každého zaměstnance zvlášť, což umožňuje srovnat výkonnost zaměstnanců v čase. Aplikace také přímo na domovské stránce nabízí přehledný dashboard, na kterém jsou data vizualizovaná s pomocí různých typů grafů. Vkládání nových záznamů probíhá buď v samostatném separátním okně, nebo přímo v tabulce (má-li uživatel dostatečná oprávnění). Data jsou zadávaná jak samotnými zaměstnanci, tak jejich nadřízenými a výstupy z této aplikace slouží

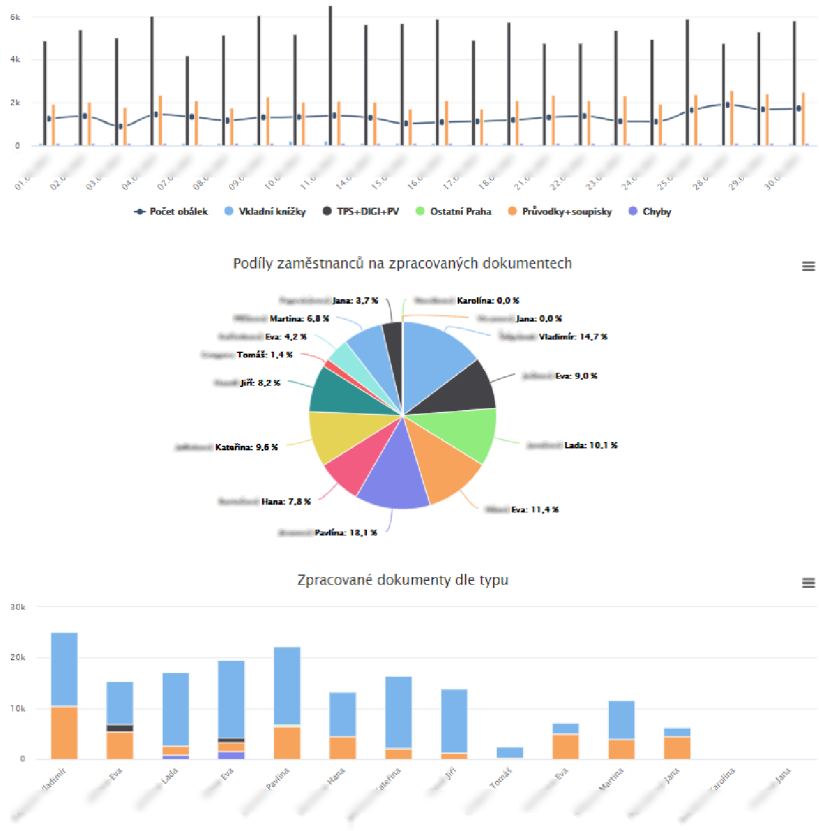
jednak jakožto podklady pro fakturaci zákazníkovi (spol. ČSOB), která si vede vlastní kontrolní součet, ale také pro porovnání výkonnosti zaměstnanců, které probíhá primárně na týdenní bázi.



Obrázek č. 31: Uživatelské prostředí Aplikace Třídírna
(Zdroj: autor)

Aplikace nabízí pokročilé možnosti filtrování – dle data, zaměstnance, doby na pracovišti apod. a umožňuje také snadný export dat do schránky či ve formátu MS Excel, CSV nebo PDF. Funkce exportu do Excelu nyní využívá pověřený pracovník, který každý týden data stahuje pro pokročilejší analýzu v prostředí MS Excel.

Přidání nového pracovníka třídírny se provádí na kartě „Zaměstnanci“, kde je nutné vyplnit jeho jméno, příjmení, mzdové údaje a úvazek. Výpočetní sloupec pak automaticky dopočítá přibližné hodinové náklady na daného zaměstnance. Provozní tabulka pak nabídne přiřazení zaměstnance z tabulky zaměstnanců v této relační databáze. Obdobně funguje i „Nastavení“, kde se zadávají hodnoty jednotlivých operací či úkonů.



Obrázek č. 32: Část dashboardu Aplikace Třídírna
(Zdroj: autor)

Uživatelé aplikace, kterých je nyní přibližně 7 , mají rozdílné role. Aplikace podporuje tři základní typy uživatelských účtů v závislosti na udělených oprávněních. Jedná se o následující role:

- administrátor
- manažer
- zadavatel

Administrátor má k aplikaci servisní přístup, což umožňuje nastavování některých parametrů, které není možné konfigurovat z frontendu. Manažerům je umožněn přístup k exportům a mohou zadaná data upravovat (byť je zde samozřejmě historie změn vč. monitoringu přihlášení). Zadavatel, tj. nejnižší úroveň oprávnění umožňuje po přihlášení do aplikace pouze zadávat denní data za jednotlivé zaměstnance (někteří si je zadávají sami). Karty „Zaměstnanci“ ani „Nastavení“ nejsou s tímto uživatelským oprávněním přístupné. Také možnosti editace tabulky jsou značně omezené a zadané údaje staršího data jsou pak pouze pro čtení, aby se zabránilo případné (úmyslné či

neúmyslné) manipulaci s daty evidovanými v systému. Data v této aplikaci jsou uložena v databázi MySQL u poskytovatele hostingu. Databáze je zálohovaná na denní bázi u providera a jiné zálohování (např. lokální) na pravidelné bázi neprobíhá.

Mezi nedostatky této aplikace patří občasné pomalé načítání, což je zřejmě dáno výchozími možnostmi server-side processingu v rámci sdíleného hostingu. Grafy na domovské obrazovce však podporují pouze výchozí řazení dle údajů v tabulce a neumožňují interaktivní filtrování – vždy tedy podléhají zobrazené tabulce. Hodnoty v grafech tak často nejsou řazeny dle velikosti, což má u některých souhrnných grafů problematickou vypovídající hodnotu. Zejména z tohoto důvodu je proto nutný export do MS Excel pro další zpracování pravidelných reportů, jelikož možnosti operaci s daty jsou přímo v aplikaci poměrně omezené.

Případná nedostupnost či nefunkčnost aplikace by nepředstavovala významný zásah do fungování organizace, jelikož tato aplikace není pro chod podniku kritická. Bylo by však nutné přejít na značně komplikovanější systém ruční evidence většího množství dat a jejich následné analýze v prostředí MS Excel.

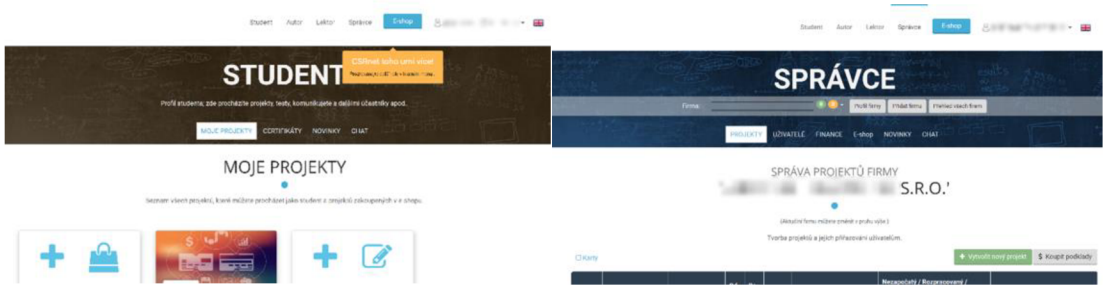
3.3.2.4 CSRnet

CSRnet je komplexní systém rozvoje lidských zdrojů, resp. zaměstnanecký podnikový portál, který zahrnuje oblasti jako je školení zaměstnanců, jejich testování, realizace průzkumů nebo systém distribuce benefitů. V souvislosti s CSRnetem je nutné zmínit i jeho stejnojmenného předchůdce, z něhož vycházejí požadavky na současný systém.

Obrázek č. 33: Logo aplikace CSRnet
(Zdroj: autor)

Potřebu použití nějakého software, který by obsáhnul některé procesy zaměřené na práci se zaměstnanci společnost identifikovala, slovy jejího ředitele, již na konci roku 2018. Některé činnosti už nešlo dělat „stylem tužka papír“ – realizace školení se zadávala externím dodavatelům, testování a průzkumy probíhaly povětšinou v listinné podobě. Firma také chtěla umožnit svým zaměstnancům, aby na této platformě mohli zároveň odpovídat na četné dotazníky (průzkumy spokojenosti apod.) a později se k požadavkům na systém přidal i „e – shop“ se zaměstnaneckými benefity. Jelikož

žádný takto komplexní systém na trhu nebyl, nebylo jej možné nikde zakoupit, resp. customizovat na potřeby a požadavky sociální firmy. Podnik proto šel cestou vývoje na míru od externího dodavatele – o necelý půlrok později bylo zahájeno výběrové řízení a vybraná společnost započala vývoj aplikace. Tento dodavatel ovšem nebyl schopen vývoj dokončit ve smluvené lhůtě dle harmonogramu realizace, a proto jej společnost nechala doprogramovat za pomocí jiného dodavatele. Vývoj aplikace trval déle než rok, přičemž náklady se pohybovaly v řádech nižších jednotek milionů korun. Firma vývoj této aplikace nezamýšlela pouze pro vlastní použití, ale kalkulovala i s cílem prodávat ji jakožto produkt dalším (nejen) sociálním podnikům. Vývoj byl dokončen na přelomu let 2019 a 2020 a vznikla tak standalone webová aplikace tehdy poprvé pojmenována označením CSRnet. Firma také společně s finální aplikací obdržela, v souladu s licenčním ujednáním, i veškeré zdrojové kódy. Záměr využít jej jakožto produkt se zhodnotil poměrně brzy, když se podařilo prodat několik licencí společnostem zaměstnávající vysoký podíl OZP pracovníků. Tehdy se také zamýšlelo vyvinout multiplatformní mobilní aplikaci, z čehož však nakonec z řady důvodů sešlo.



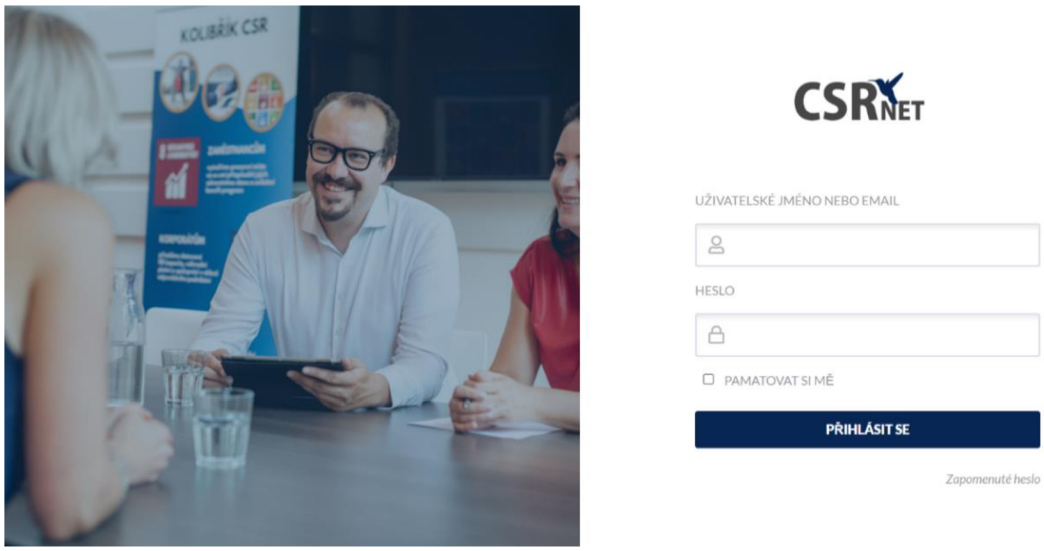
Obrázek č. 34: Vzhled uživatelského rozhraní původní aplikace CSRnet
(Zdroj: autor)

S implementací původního systému se v podniku započalo v první polovině roku 2020. Nejprve se začalo s testováním skupinou zaměstnanců, hned v počátku však bylo zjištěno například nefunkční generování certifikátu v případě, kdy bylo testování podmíněno ještě přiložením jistých nutných příloh. Zhotovitelská firma nebyla schopna bezmála půl roku chybu najít a opravit. Systém se také nejevil stabilní při zátěžových testech, kdy se do něho přihlásilo více jak 50 uživatelů naráz. Postupně se začalo kumulovat množství nedostatků a problémů způsobených touto aplikací. Kritika přicházela i ze strany zaměstnanců, kteří aplikaci vyčítali nejen funkčnost, ale i její uživatelské prostředí, které nebylo příliš intuitivní a špatně se v něm orientovali. Největším problém však bylo zjištění, že aplikace byla prakticky nepoužitelná na

mobilních zařízeních. Společnost tak ihned vznesla požadavek na redesign, avšak v průběhu času došlo k selhání dalšího dodavatele, který navíc poukazoval na špatně specifikované podmínky při návrhu aplikace. Do této situace začala společnost řešit strategické změny ve společnosti a její dělení následované po odprodeji části firmy (call-centrum) a vznik nových subjektů. Započal tak přerod malého podniku ve větší firmu a zástupci společnosti tak celý plán přehodnotili. Nakonec tak z celopodnikové implementace zcela sešlo a z původní aplikace zůstal pouze produkt, jenž prošel rebrandingem (např. Proxnet) a byl poskytnut několika dalším podnikům, což částečně pomohlo kompenzovat relativně vysoké pořizovací náklady za tento IS na míru.

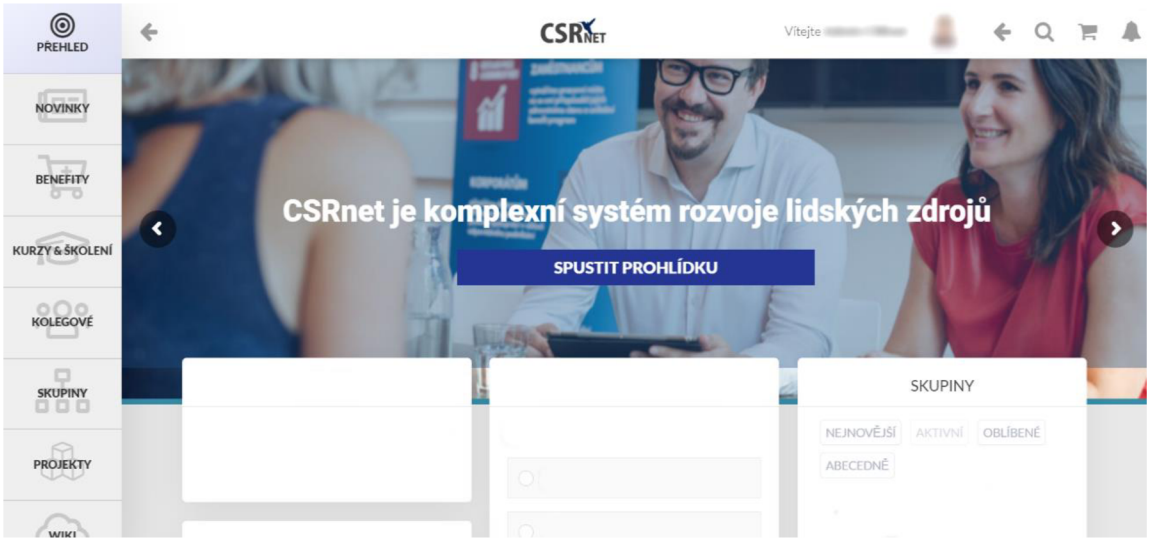
Po určité době, co se situace ve společnosti částečně stabilizovala, začala v podniku opět sílit potřeba tohoto systému, což po dlouhých úvahách o modifikaci a redesignu původního systému dalo nakonec vzniknout nové, stejně pojmenované aplikaci na zcela jiné platformě, jejíž vývoj je v současné době (jaro 2022) zcela novým dodavatelem právě dokončován. Ačkoliv byl tento systém také prakticky na míru, byl paradoxně výrazně levnější. (Pozn.: Porovnáváme-li oba systémy ve stejné fázi životního cyklu, tj. nejsou zde zatím známy žádné vícenáklady plynoucí např. z implementačního procesu, vyjma požadavku na schopnost distribuce výplatnic.) Tento nový CSRnet navíc oplývá moderním designem, ještě více modulárním provedením, splňuje pravidla přístupnosti (např. režim vysokého kontrastu) zvlášť akcentované u sociální firmy zaměstnávající osoby zdravotně postižené (mnohdy např. slabozraké), a co víc – obsahuje i moderní prvky sociální sítě na rozdíl od předchozího systému, který měl podobu spíše e – learningu doplněného o možnost nákupu položek. Tento systém nabízí celkově více možností přizpůsobení a konfigurace a plní více úlohu interní komunikační platformy. Nová aplikace také ve velké míře pracuje s gamifikací a podporuje interaktivní kvízy a školení v rámci HTML5. Gamifikace zde úzce souvisí s konceptem bodového konta, jakousi virtuální elektronickou peněženkou, prostřednictvím které bude zaměstnancům distribuována část benefitů. Ti si tak budou moci sami vybrat a objednat zvolený benefit z interního e – shopu, což jednak značně urychlí celý proces distribuce benefitů (který je v současné době řešen telefonicky nebo zasláním e – mailu na speciálně zřízenou mailovou adresu) a uspoří personální náklady, avšak také bude jednodušší pro většinu samotných zaměstnanců. Tato forma distribuce se přímo nabízí, jelikož se nyní často jedná zejména o elektronické kupony či poukazy (masáže, kino, ad.).

Tato aplikace není v současné době (jaro 2022) ještě zcela dokončena a připravena ke spuštění, jelikož se na ní stále dolaďují poslední práce. Avšak odhaduje se, že cíle, tj. nahrazení stávajícího systému (tzn. z části ruční, z části využívání mnoha aplikací třetích stran) podaří dosáhnout nejpozději do začátku roku 2023. Součástí této práce bude tedy sestavení základního plánu implementace této aplikace.



Obrázek č. 35: Přihlašovací obrazovka aplikace CSRnet
(Zdroj: autor)

Pro CSRnet je charakteristický jednotný vizuální styl totožný s webovými stránkami společnosti (www.kolibrikcsr.cz). Samozřejmostí je také plně responzivní design umožňující pohodlné ovládání prostřednictvím mobilních zařízení, což předchozí systém nenabízel. Domovská obrazovka je vybavena systémem interaktivních widgetů, což nabízí mnohem širší možnosti customizace na míru každému uživateli. Téměř vše je intuitivní a dá se ovládat také přetáhnutím (drag and drop).



Obrázek č. 36: Ukázka uživatelského rozhraní aplikace CSRnet
(Zdroj: autor)

V základu aplikace podporuje minimálně tři uživatelské role – vyjma administrátora, který má jako jediný možnost například přeskupovat nabídku základního menu, se zde nacházejí manažeři a uživatelé. Manažeři mohou spravovat kurzy nebo měnit nabídku benefitů. Tyto role se liší také například možností přispívat do integrované znalostní báze nebo přidávat novinky. Portál je primárně zaměřen na zaměstnance, ale funkcionality nabídne i manažerům – například základní nástroje projektového řízení. Jedná se tedy o skutečně zcela komplexní systém pro vzdělávání, testování, komunikaci a distribuci benefitů jehož uživateli budou výhradně zaměstnanci společnosti. Jedná se o cloudovou webovou aplikace, která je však schopná běžet i v rámci firemního intranetu.

Vzhledem k široké škále nabízených funkcionalit centralizovaných na jednom místě lze tuto aplikaci označit jako podnikový portál, resp. zaměstnanecký podnikový portál (někdy též označován B2E – *Business to Employee*). Systém je navržen tak, aby poskytoval funkcionality v následujících okruzích procesů:

- **Školení** – systém bude sloužit ke školení všech zaměstnanců na bezpečnost práce, požární ochranu, školení řidičů, ale i ke školení kompetencí nutných k výkonu práce na jednotlivých odděleních – ať už školení na speciální SW jejich klientů, ve kterých jejich zaměstnanci mnohdy pracují, nebo obecně ke zvyšování jejich kompetencí,
- **Testování** – nejen školené osoby je možné testovat na celou paletu otázek – testování bude používáno na ověření jejich kompetencí např. na odděleních, kde

jsou vysoké nároky na kontinuální doplňování znalostí (např. oddělení Finančních trhů),

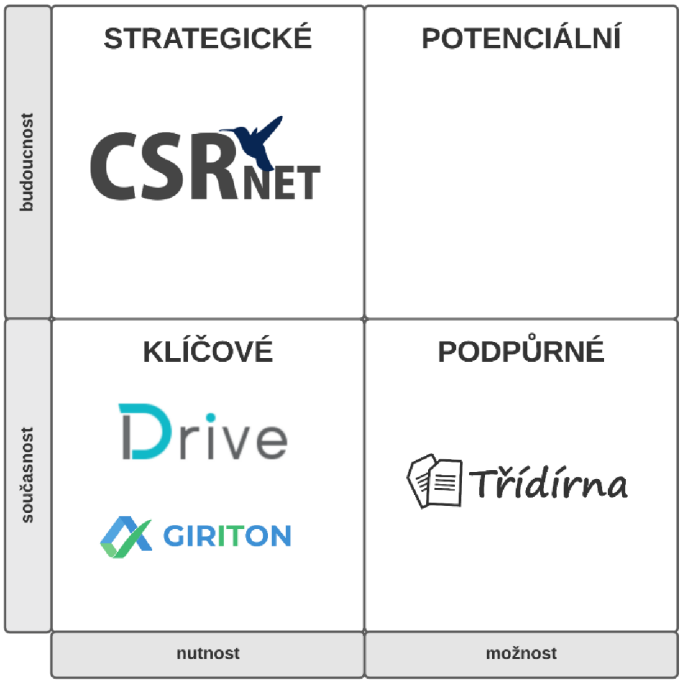
- **Benefitní systém** – elektronická peněženka u každého zaměstnance umožňuje distribuci benefitů přesně na míru každého z nich (část benefitů bude tedy distribuována formou dobití „kreditů“ do této peněženky),
- **Průzkumy** – jako sociální firma se sales24, s.r.o. pravidelně zajímá o názory svých zaměstnanců, které budou zjišťovány mimo jiné i prostřednictvím této platformy, nebude tedy nutné využívat služby třetích stran jako například Survio (jedná se např. průzkumy na téma atraktivity různých benefitů, nebo koho podpoří firma z tzv. Colibri fondu, kde bude vánoční večírek, jak vnímají svoje nadřízené, co by chtěli zlepšit na pracovišti apod.).

Společnost si od zavedení tohoto systému slibuje mimo jiné podporu skupinové interakce, resp. posílení komunikace, jelikož Kolibříci jsou často rozmístěni napříč městy, pobočkami a odděleními, a tím i posílení firemní kultury.

Systém by dle posledních požadavků (jaro 2022) měl umožňovat také distribuci výplatních pásek k zaměstnancům a nahradit tak jejich nynější rozesílání e – mailem jakožto zaheslovaných příloh. Tato funkcionalita však nebyla představiteli podniku specifikována při zadávání poptávky a formulování požadavků na systém. Nic však nyní nenasvědčuje tomu, že by to bylo technicky nemožné a zvlášť výrazně finančně nákladné. V budoucnu by do něho mohl být zaintegrován i docházkový modul, aby se naplno využila komplexnost portálového řešení.

3.3.3 McFarlanův model

Tento model aplikačního portfolia kategorizuje podnikový software dle přínosů jednotlivých aplikací pro podnik z pohledu jejich důležitosti a času, resp. současnosti i budoucnosti. Většina procesů využívajících IS se v podniku týká zejména personalistiky i z tohoto důvodu není aplikační portfolio společnosti příliš různorodé.



Obrázek č. 37: McFarlanův model aplikačního portfolia
(Zdroj: autor)

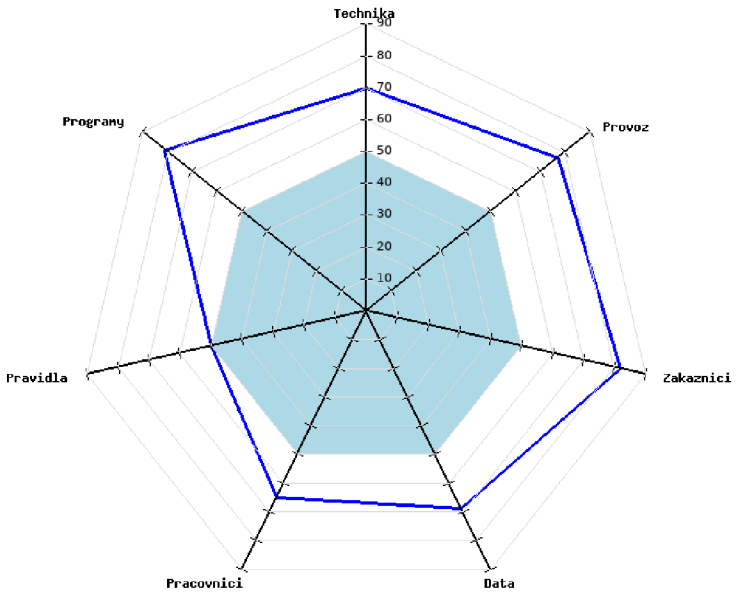
V modelu nejsou uvedeny běžně používané kancelářské aplikace, stejně jako komunikační aplikace zmíněné v textu výše. Tyto by byly zahrnuty do sektoru podpůrných aplikací. Mezi stávající aplikace nutné k provozu, tedy ty klíčové, je nutné zařadit Synology Drive a Giriton, byť v případě druhé zmiňované aplikace by bylo možné uvažovat i o zařazení do sektoru podpůrných aplikací, kam jednoznačně spadá BI Aplikace Třídírna. Přínosy této podpůrné aplikace jsou také relativně snadno měřitelné, jelikož nahradila zdlouhavou ruční evidenci úkonů a slouží také k porovnávání pracovní výkonnosti zaměstnanců třídírny v Hradci Králové. Synology Drive v současnosti usnadňuje výměnu informací (zvl. z oblasti personalistiky) mezi manažery, resp. mezi jednotlivými pobočkami a pracovišti, a tak zvyšuje produktivitu práce, avšak její potenciál, resp. potenciál NAS Synology není ještě zdaleka vyčerpán. Aplikace Giriton se nyní využívá ke svému primárnímu účelu, tj. k evidenci a vykazování docházky a plánování směn. Nový komplexní portál CSRnet je jednoznačně strategickou aplikací, která má značný potenciál stát se klíčovou aplikací v podniku, pokud se její implementace vydaří. CSRnet umožní zefektivnit široký okruh procesů týkajících se zaměstnanců – od vzdělávání zaměstnanců až po distribuci výplatnic i benefitů.

3.3.4 Metoda ZEFIS

K auditu informačního systému byla využita webová aplikace ZEFIS. Pomocí ZEFIS je možné posuzovat jednotlivé procesy v kontextu celého IS, což je výhodné zvláště v případě větších společností s více odděleními, rozsáhlým informačním systémem a jednoznačně zmapovanými procesy. V tomto případě je hlavní náplní práce administrativní činnost, přičemž zákazníci IS jsou takřka výhradně vnitropodnikoví. Výstupem auditu informačního systému je vždy celkový audit firmy, hodnotí se vždy efektivnost užití určitého informačního systému v daném procesu stejně jako jeho bezpečnost. Jednotlivé dotazníky byly vyplňovány společně s kompetentními osobami – tj. např. s jednatelem společnosti, jenž má oblasti IS/IT ve své gesci nebo s provozní ředitelkou.

3.3.4.1 Efektivnost IS

Efektivnost neboli účelnost obecně vyjadřuje stupeň dosažení určitého předem stanoveného cíle – v tomto případě vhodně vybraných, korektně nastavených a správně provozovaných informační systémů a bezchybných procesů podniku. K teoretické hranici 100 % se v praxi podniky málokdy přiblíží.



Graf č. 1: Efektivnost IS zkoumané firmy v procentech
(Zdroj: ZEFIS)

Na grafu je patrný odhad efektivnosti dle jednotlivých zkoumaných dílčích oblastí. Celková efektivnost užití IS v daném podniku je vždy rovna nejnižší z dílčích hodnot. Za systém s vysokou efektivností je považován jen vyvážený systém, kde mají všechny oblasti přibližně stejnou efektivnost. Takovéto řešení má obvykle nejnižší náklady a vysokou účinnost.

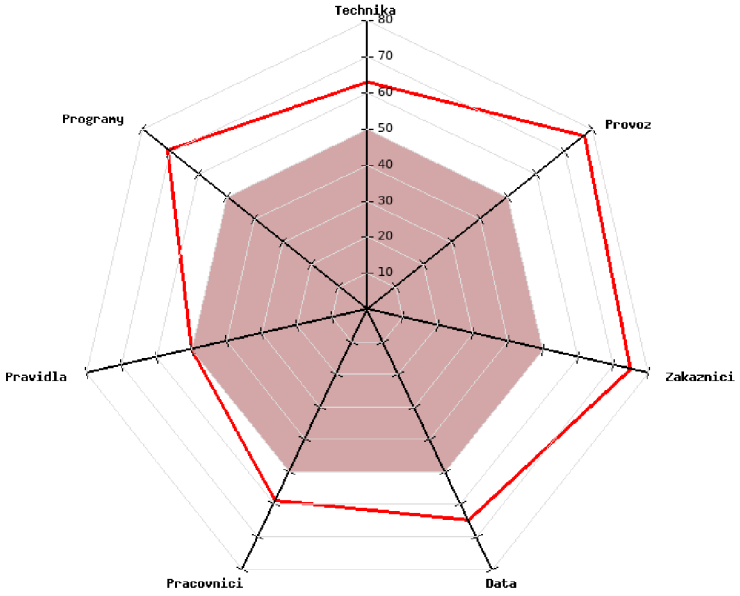
Tabulka č. 2: Efektivnost IS zkoumané firmy dle oblastí
(Zdroj: ZEFIS)

Oblast	**Stav**
Pravidla	50 %
Pracovníci	65 %
Data	69 %
Technika	70 %
Provoz	77 %
Programy	81 %
Zákazníci	82 %
Celkem	**50 %**

Pokud je efektivnost některé z oblastí rovna 50 %, znamená to, že veškeré testované best practices byly porušeny, což je v tomto případě oblast Pravidel. Dosažení 100 % by naopak znamenalo plnou shodu s ideálním stavem pro daný typ firmy.

3.3.4.2 Bezpečnost IS

Bezpečnost nemůže být řešena pouze pro jeden informační systém, ale řeší se vždy pro celou firmu, včetně všech procesů a systémů. Analogicky jako u efektivnosti platí, že celková bezpečnost IS je dána vždy úrovní nejslabší oblasti.



Graf č. 2: Bezpečnost IS zkoumané firmy v procentech
(Zdroj: ZEFIS)

Z grafu jsou patrné výrazné nedostatky zejména v oblastech Pravidel a Pracovníků. Výsledek 50 % v případě oblasti Pravidel indikuje, že všechny testované bezpečnostní zásady jsou v podniku porušeny.

Tabulka č. 3: Bezpečnost IS zkoumané firmy dle oblastí
(Zdroj: ZEFIS)

Oblast	**Stav**
Pravidla	50 %
Pracovníci	59 %
Technika	63 %
Data	65 %
Programy	71 %
Zákazníci	75 %
Provoz	77 %
Celkem	**50 %**

Oblast pravidel limituje celkový stav, avšak i výsledky ostatních oblastí značí, že systém je i z hlediska bezpečnosti nevyvážený. Zejména zlepšení v oblasti Pravidel se promítne i do zvýšení bezpečnosti potažmo i efektivity celého informačního systému podniku.

3.3.4.3 Identifikace nedostatků

Níže jsou uvedeny nejzávažnější nedostatky, tj. ty s významností „vysoká“, identifikované metodou ZEFIS. Pozn.: Šedě jsou podbarveny ty nedostatky, které nemají přímý vliv na bezpečnost IS.

Tabulka č. 4: Nejvýznamnější identifikované nedostatky
(Zdroj: vlastní zpracování dle ZEFIS)

Oblast	Nedostatek
Pravidla	Chybí manažer/ka informačních systémů
Pravidla	Chybějící, nebo špatně dodržovaná bezpečnostní pravidla
Data	Nejsou zálohována data na počítačích pracovníků
Programy	Pracovníci mohou instalovat programy na své počítače
Pracovníci	Nedodržování pravidel
Pravidla	Chybí informační strategie
Pravidla	Chybí strategie bezpečnosti
Data	Chybějící metodika zálohování dat
Provoz	Bezpečnostní hrozba přístupu do podnikové sítě
Technika	Slabší obrana proti útokům v počítačové síti
Pravidla	Zodpovědnost za likvidaci dat, datových nosičů
Pravidla	Chybí manažer/ka informační bezpečnosti
Pravidla	Chybí klasifikace dat/informací
Pravidla	Špatně stanovená zodpovědnost pracovníků v procesu
Pravidla	Nejsou pravidla a postupy, jak se provádí proces
Zákazníci	Neprobíhají bezpečnostní školení uživatelů IS pracujících s daty zákazníků
Technika	Špatné fyzické zabezpečení klíčových prvků infrastruktury
Pravidla	Chybí bezpečnostní pravidla informačního systému
Pracovníci	Přístupová práva zaměstnanců nejsou správně ukončována
Pracovníci	Nastavení přístupových práv
Pracovníci	Není vytvářeno bezpečnostní povědomí pracovníků
Pracovníci	Neprobíhají periodická bezpečnostní školení uživatelů IS
Pracovníci	Nejsou aktualizovaná hesla uživatelů
Pracovníci	Přístupová práva zaměstnanců nejsou včas nastavována
Pracovníci	Pracovníci neznají pravidla pro práci s informačním systémem

Data	Riziko ztráty a zneužití lokálních dat
Pravidla	Chybějící, nebo nedodržovaná pravidla likvidace papírových dokumentů

Z tabulky je patrné, že se drtivá většina identifikovaných významných nedostatků týká zároveň i bezpečnosti, přičemž nejvíce negativních zjištění se týká oblasti Pravidel a Pracovníků. V podniku chybí informační strategie, což je scénář, ve kterém jsou formulované podnikové vize a stanovené podnikové cíle. V informační strategii je definováno, jakých informačních systémů a jaké techniky je třeba pro dosažení daných podnikových cílů, přičemž je třeba postupovat systematicky. Podniková informační strategie by ideálně měla mít formalizovanou podobu písemného dokumentu.

S informační strategií úzce souvisí i strategie bezpečnosti, která představuje postup, jak dosáhnout nejen zabezpečení informačních systémů, ale také fyzické bezpečnosti s cílem snížit riziko ztráty či zneužití dat. Za tímto účelem je vhodné pořádat periodická bezpečností školení, která v podniku neprobíhají, jelikož bezpečnost se v průběhu času snižuje není-li systematicky vyžadována a vynucována. V podniku chybí tlak ze strany vedení a nebuduje se bezpečností povědomí uživatelů, kterým je třeba připomínat rozličné hrozby a možné následky. Tato problematika je hrubě podceňována zvláště u menších podniků, kde chybí role manažera informační bezpečnosti, jenž by definoval pravidla týkající se bezpečnosti a zajišťoval jejich kontrolu a dodržování. Pro podniky totiž problematika bezpečnosti nepřináší zisk, avšak značně snižuje možná rizika. Tuto agendu je možné částečně outsourcovat na externí dodavatele. Dbát na pravidla provozu z hlediska bezpečnosti je však úkolem manažerů a nedodržování těchto pravidel bývá způsobeno špatným řízením z jejich strany. Nestačí pouze zaměstnance proškolit, ale je třeba dodržování pravidel kontrolovat a vymáhat. Nejhorší variantou je systematické tolerování jejich porušování, což ilustruje špatné fungování podniku. Vytvářet bezpečnostní povědomí pracovníků znamená pravidelně jim připomínat bezpečnostní zásady a rizika plynoucí z používání ICT, proto je bezpodmínečně nutné, aby se bezpečnostní školení konala na pravidelné bázi. Spektrum hrozeb je velmi široké a je nutné mezi ně zahrnout i aktuální trendy, jelikož IT hrozby se vyvíjí v čase. Zaměstnancům musí být připomínány hlavní bezpečnostní zásady, jimiž se musí při výkonu činnosti řídit – např. zachovávat zásadu prázdného stolu a odhlášeného počítače při jakémkoli odchodu z pracoviště, chránit si svoje hesla (což souvisí s podnikovou

politikou hesel) a zabezpečení pracovních stanic. Obsahují-li počítače citlivé údaje, chránit je odpovídajícím způsobem (např. je šifrovat).

Nedostatečná je i fyzická ochrana techniky – tj. zabránit přístupu nepovolaných osob. Fyzický přístup k ICT je nezbytné chránit a hlídat stejně, jako zabezpečení podnikové sítě. Povolovat cizím osobám přístup do vnitropodnikové sítě je značný hazard, jelikož je zde nemalé riziko odcizení dat či napadení sítě, zvlášť v případech, kdy je firewall nedostatečný. Počítače jsou obecně zabezpečeny poměrně obstojně, mají-li funkční antivirus, jehož je firewall obvykle součástí. Firewall monitoruje komunikaci a v případě pokusu o neoprávněný či podezřelý přístup tuto komunikaci terminuje. Obdobná funkce na dalších síťových zařízeních jako jsou routery nebo servery je povětšinou stranou zájmu, stejně jako v tomto případě. Možnost zaměstnanců instalovat na své počítače libovolné programy je pak problém jak z pohledu bezpečnosti, tak možné instalace ilegálního softwaru (warez) a z toho plynoucích důsledků.

Ve firmě neexistuje metodika zálohování dat, která by definovala a předepisovala kdo, kdy, co (což vyžaduje provést soupis dat, která jsou pro podnik důležitá) a především kam zálohuje. Obecně přitom platí zásada, že rozdíl mezi zálohou a skutečným stavem by neměl být větší než objem jednodenní práce. V podniku také není určena osoba odpovědná za likvidaci dat, resp. datových nosičů (potenciálně) obsahující citlivá data, což může způsobit únik informací. Je třeba definovat postupy, a především pak provést klasifikace dat dle jejich citlivosti, resp. důvěrnosti.

Je nutné, aby byla zajištěna náležitá ochrana elektronických dat a s ohledem na ni nastavovat přístupová pravidla do systémů. Ve společnosti také nefungují pravidla ohledně likvidace listinných dokumentů, resp. nejsou stanovena nebo dodržována. S tím souvisí i pravidla skartace. V současnosti je třeba naplňovat aktuální legislativní požadavky – například data o zákaznících podléhají ochraně dle GDPR. V případě elektronických médií je povětšinou nestačí pouze smazat, jelikož mohou být obnovena, pokud nebyla přepsána jinými daty. I tuto agendu je možné do určité míry outsourcovat, je však potřeba ji řešit.

Metoda ZEFIS odhalila i špatné vykonávání procesů, což souvisí s jejich nepříliš dobrým nastavením napříč podnikem. Pro každou činnost je nutné definovat zodpovědného konkrétního pracovníka či roli, což je možné znázornit např. pomocí

RACI matice. Nemělo by se stávat, aby za daný proces zodpovídali dva pracovníci (či více) nebo naopak nikdo. V této souvislosti je třeba říci, že je nutné výrazným způsobem zlepšit řízení, což klade důraz na přístup managementu v této oblasti. Pravidla a postupy, jak se určitý proces provádí, nemusí být vždy nutně formulovány písemně, ale je důležité, aby je dotčení pracovníci vždy přesně znali, a především se jimi řídili. Jakmile se podnik zvětšuje, neobejde se bez písemných postupů a formalizovaných směrnic, které je třeba aktualizovat, dodržovat a především, jak již bylo zmíněno výše, kontrolovat.

Příkladem špatně nastaveného procesu a závažným rizikem je například neukončování přístupových práv zaměstnanců při jejich odchodu. Včasného zrušení přístupu se docílí zejména vhodným nastavením předávání informací. Tento vhodně nastavený proces vyžaduje součinnost správce IT, resp. správce přístupových práv a personálního oddělení. Pracovníci většinou chybějící práva připomínají a urgují, avšak opačně tomu většinou tak nebývá.

Mezi další identifikované nedostatky patří zejména neexistence záložního technického řešení a plánů na obnovu dat, což souvisí s faktem, že chybí také směrnice pro řešení havarijních situací. V podniku je také nevhodný způsob likvidace nosičů dat i celých zařízení obsahující paměťová média, ale také špatně nastavené pracovní postupy a problémové procesy. Je zde přítomna bezpečnostní hrozba plynoucí z přístupu na internet a riziko zneužití dat, popř. virového útoku. Neexistují formalizované pracovní postupy a pravidla pro práci s informačním systémem, stejně jako chybí kontaktní místo pro hlášení závad a požadavků. Problematická je také zastupitelnost klíčových pracovníků pro IS. Z výsledků taktéž vyplývá, že je zde nespokojenost pracovníků s technickou podporou (vč. pomalé doby odezvy) a není zajištěna systematická uživatelská podpora. Pracovníci by také nejspíše uvítali školení ohledně IS.

3.3.5 Primární výzkum informační bezpečnosti

Snaha o zjištění stavu informační bezpečnosti v podniku je zejména reakcí na nalezené potenciálně problematické oblasti v oblasti bezpečnosti IS, zvlášť pak v oblasti Pravidel a Pracovníků, pomocí metody ZEFIS při posuzování celého informačního systému podniku.

3.3.5.1 Metodologie výzkumu

Cílem primárního výzkumu je zhodnocení stavu informační bezpečnosti ve společnosti sales24, s.r.o. z pohledu vybraných klíčových pracovníků a návrh změn vedoucích ke zvýšení informační bezpečnosti podniku (Novotný, 2022). Je nutné zdůraznit, že tento výzkum se soustřeďuje výlučně na zhodnocení stavu informační bezpečnosti v těch částech informačního systému a těch uživatelů informačního systému, kteří nepracují v systémech klientů. Je tedy zaměřen primárně na pracovníky administrativního týmu a managementu. Řadoví pracovníci pracují povětšinou v systémech, na technice (hardware) a v rámci bezpečnostních politik klientů (typicky bankovních institucí), jejichž stav informační bezpečnosti se může značně lišit a zpravidla se také výrazně liší.

Centrální výzkumná otázka má následující podobu: *„Jaký je stav informační bezpečnosti ve společnosti sales24, s.r.o.?“*

Obrázek č. 38: Metodologie výzkumu
(Zdroj: autor)

Základním východiskem tohoto výzkumu je tedy aplikace metody ZEFIS na informační systém užívaný ve společnosti sales24, s.r.o. (Kolibřík CSR). Na základě výsledků zhodnocení IS jsou vybrány dílčí oblasti, resp. stanoven rozsah, čím se bude předmětný výzkum zabývat. Následně dojde, po formulaci základních otázek, k realizaci rozhovorů s klíčovými pracovníky firmy. Výstupem bude výsledné zhodnocení stavu informační bezpečnosti podniku a formulace návrhů doporučení pro nápravu nejvýznamnějších identifikovaných nedostatků. Jedná se tedy primárně o deskripci stavu informační bezpečnosti v podniku. Za účelem co nejpřesnějšího zodpovězení výzkumné otázky byl

zvolen přístup kvalitativní, deduktivně-induktivní (proběhne tedy dedukce základních oblastí informační bezpečnosti a indukce konkrétních podoblastí ve společnosti z realizovaných rozhovorů). Technikou sběru dat je realizace individuálních částečně strukturovaných rozhovorů (pochopitelně se souhlasem respondentů vždy nahrávaných). Účastníci rozhovoru byli vybráni kvalitativním vzorkováním, resp. metodou záměrného výběru – byly identifikovány klíčové osoby, které jsou pro předmět výzkumu relevantní a jejich kompetence se určitým způsobem týkají oblasti informační bezpečnosti podniku.

Identifikace klíčových pracovníků byla relativně problematická, jelikož na základě prvotního seznámení se společností bylo zjištěno, že společnost nemá jasně definované role, co se týká bezpečnosti či IT, a už vůbec nemá tyto role jakkoliv formálně zakotvené. Značnou část této agendy má na starosti externí IT pracovník, jedná se například o montáž hardware apod., nicméně ve specifické pozici se nachází jednatel společnosti, který neoficiálně vykonává celou řadu činností týkajících se IT, jako je například nákup a distribuce licencí k antivirovým programům a obecně lze konstatovat, že celou tuto agendu v praxi zaštiťuje.

Tabulka č. 5: Profil účastníků výzkumu
(Zdroj: autor)

Identifikace účastníka	Pozice ve společnosti	Důvod výběru (vztah k IS)
U1	Jednatel, zakladatel společnosti	Výkon správy nad značnou částí IS
U2	Vedoucí administrativního týmu, projektový manažer	Detailní znalost procesů probíhajících ve firmě
U3	Provozní ředitelka	Vedoucí provozu – nadřízená externího IT technika
U4	Obchodní ředitel	Podílel se na vytváření interních směrnic
U5	Externí IT technik (HW)	Vykonává většinu úkonů ohledně HW části IS – tj. instaluje PS, síť. tiskárny atp.

V tabulce výše je uveden důvod výběru daných účastníků rozhovoru. Jedná se o čtyři zaměstnance společnosti a jednoho externího pracovníka vykonávající činnost na dohodu o pracovní činnosti (DPČ).

Sběr dat, tj. realizace rozhovorů, probíhala v období listopadu až prosince 2021. Průměrná délka trvání rozhovoru činila přibližně 37 minut. Rozhovory byly realizovány online prostřednictvím videokonferenční platformy Jitsi. Záznam hovorů (ve 4 případech se jednalo o videohovory, v 1 případě o audiohovor) byl s výslovným

souhlasem všech účastníků ukládán do služby Dropbox, aby posléze proběhla transkripce, tj. přepis rozhovorů, prostřednictvím webové aplikace Beey.io. Tato transkripce však není ve většině případů příliš přesná a bylo nutné provést ruční korekturu všech přepisů. Zpracování analýz vč. kódování dat a tvorby myšlenkových map (MAXMapy) a tabulek proběhlo v software MAXQDA Analytics Pro 2022 (zakoupena studentská licence).

Kategorizace základních oblastí vychází primárně z InfoSec modelu. Pro účely výzkumu byly tedy na základě literární rešerše ustanoveny 3 základní oblasti informační bezpečnosti – administrativní oblast, fyzická oblast a IT oblast. Pro každou oblast byla připravena sada otázek, nicméně v závislosti na odpovědích či jiných reakcích účastníků rozhovorů byly případně položeny otázky doplňující, vysvětlující či nové.

Níže je uveden příklad otázek použitých v rozhovorech:

Administrativní oblast

- *„Jak je ve vaší společnosti řešena archivace písemných dokumentů?“*
- *„Jak je ve vaší společnosti řešena likvidace písemných dokumentů?“*
- *„Jaká jsou ve vaší organizaci bezpečnostní pravidla, předpisy či směrnice ve vztahu k bezpečnosti elektronických dat?“*

Fyzická oblast

- *„Kdo všechno má fyzický přístup k vašemu routeru a další síťové architektuře?“*
- *„Je podle vás fyzické zabezpečení prostor, kde se nachází vaše technika dostatečné?“*
- *„Jakým způsobem skladujete písemnosti?“*

IT oblast

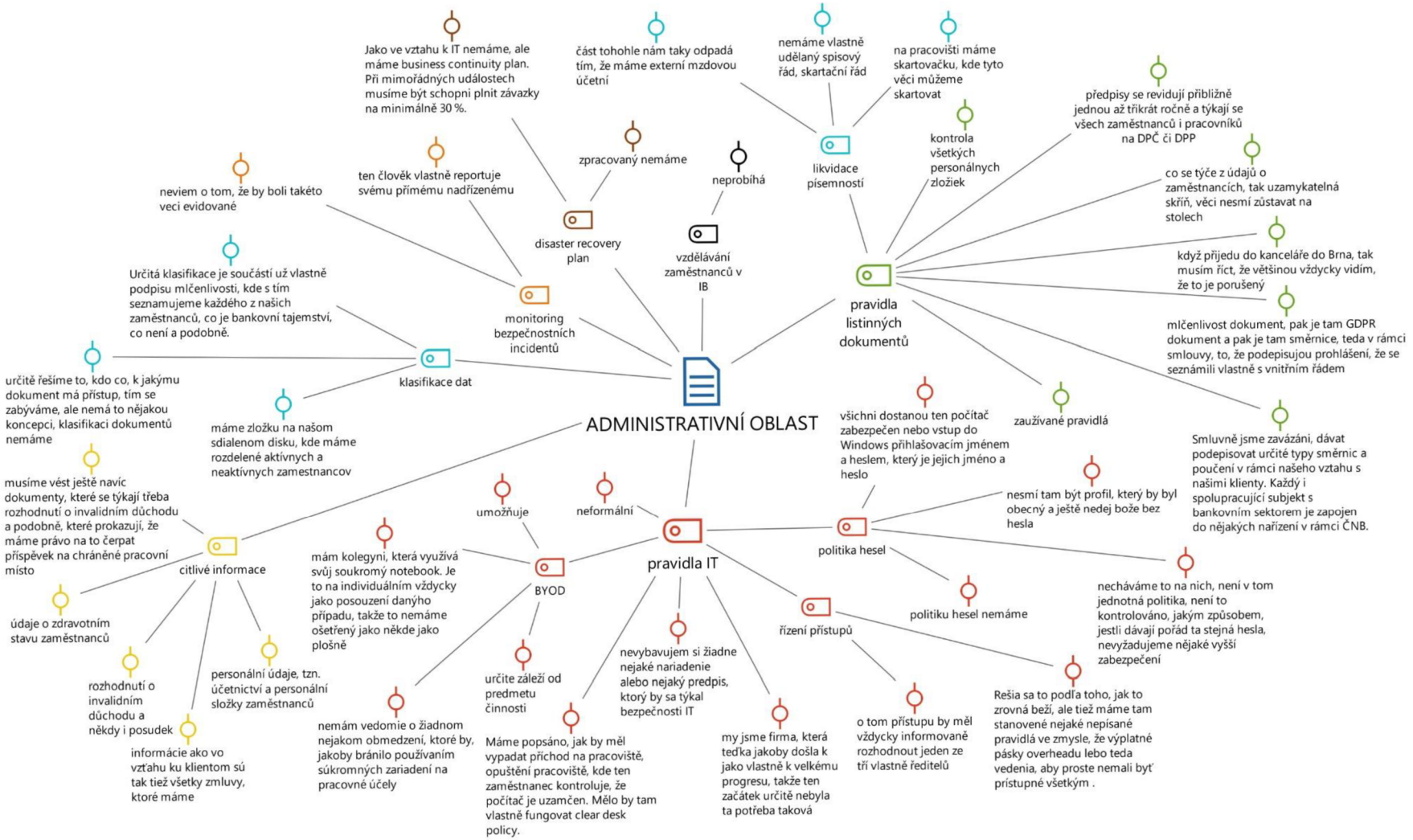
- *„Jakým způsobem probíhá likvidace vysloužilých či rozbitých elektronických médií (flash disky, HDD, ...)?“*
- *„Jak ve vaší společnosti funguje monitoring bezpečnostních incidentů?“*
- *„Jaký způsob autentizace uživatelů k pracovním stanicím je ve vaší firmě používán?“*

3.3.5.2 Analýza dat a výsledky výzkumu

Analýza dat probíhala jednotlivě dle oblastí (tj. administrativní oblast, fyzická oblast, IT oblast). Výstupy výzkumu jsou jednak shrnuty pomocí shrnujících protokolů (v podobně tabulek) a jednak prostřednictvím MAXMap, kde jsou vizualizovány vztahy mezi jednotlivými oblastmi, kódy a subkódy a úryvky z transkriptů rozhovorů.

Administrativní oblast

Administrativní oblast zahrnuje problematiku pravidel, regulí, směrnic a bezpečnostní politiky vůči všem informacím a informačním aktivům, tj. jak vůči listinným dokumentům, tak elektronickým datům. Do této oblasti patří také vzdělávání zaměstnanců ohledně informační bezpečnosti nebo politika hesel na pracovišti.



Obrázek č. 39: MAXMapa – administrativní oblast
(Zdroj: Novotný, 2022)

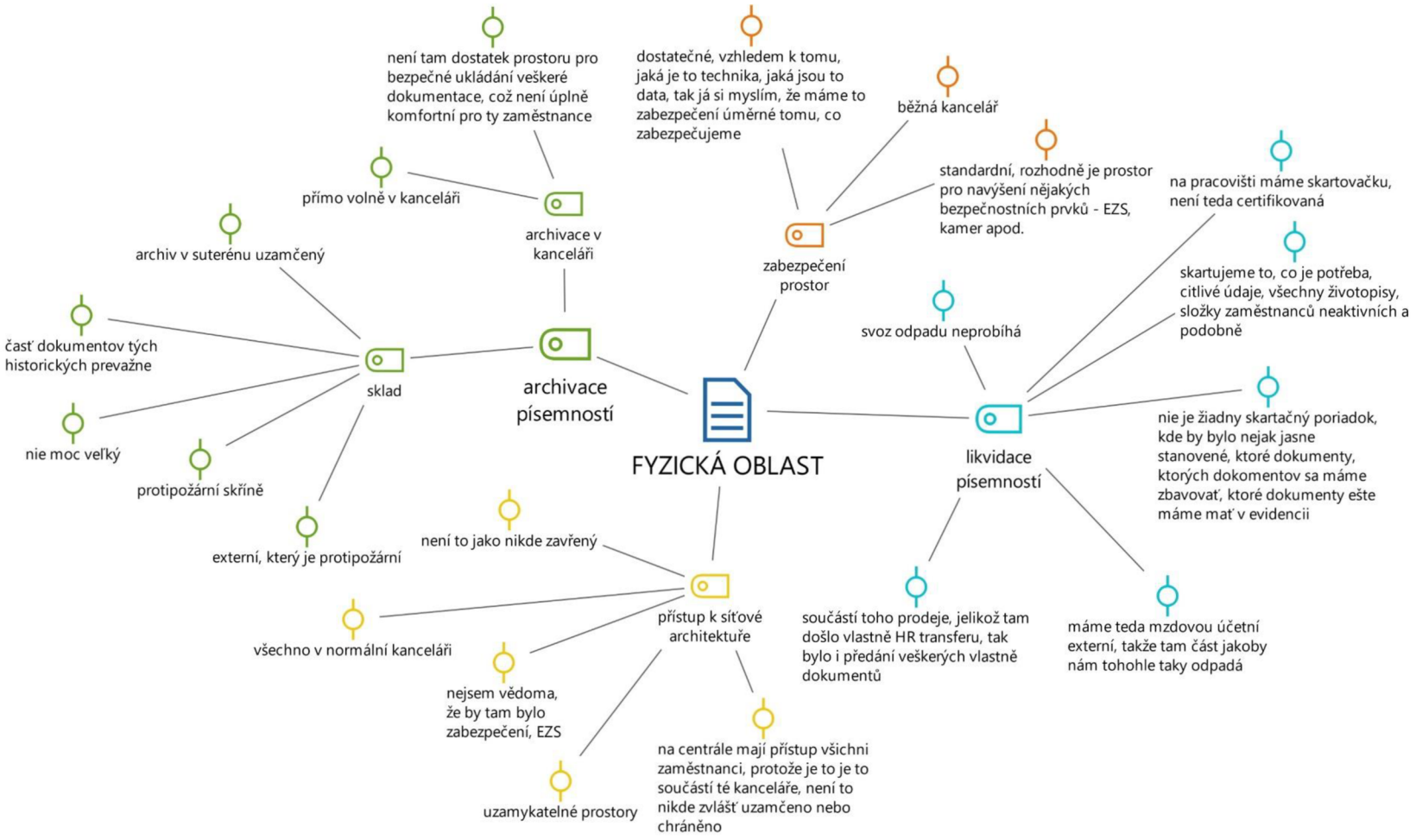
Tabulka č. 6: Shrnutí administrativní oblasti
(Zdroj: vlastní zpracování prostřednictvím MAXQDA)

Monitoring bezpečnostních incidentů	Systematický monitoring bezpečnostních incidentů v podniku neprobíhá. Hlášení případných bezpečnostních incidentů funguje standardně tak, že se pracovník obrátí na svého nadřízeného, který rozhodne, zda kontaktuje externího IT pracovníka nebo jednatele. Společnost však bezpečnostní incidenty neeviduje.
Disaster Recovery Plan	Společnost nemá zpracovaný IT Disaster Recovery Plan, nicméně existuje vypracovaný BCP (Business Continuity Plan), který je společnost povinna držet pro svého zákazníka z bankovního odvětví. Je v něm detailně popsáno, jak by podnik fungoval v případě mimořádných událostí, aby dosahoval alespoň třicetiprocentního plnění svých závazků.
Vzdělávání zaměstnanců v IB	Školení či jiné vzdělávání zaměstnanců ohledně informační bezpečnosti v podniku v žádné podobě neprobíhalo ani neprobíhá, na příští rok je však naplánován budget na vzdělávání a počítá se s nějakou formou zvyšování IT dovedností zaměstnanců.
Pravidla IT	Pravidla týkající se IT jsou spíše neformální. Je to způsobené mj. tím, že firma prošla za poslední rok velkým růstem, kdy se zněkolikanásobil počet zaměstnanců, nestal se žádný podstatný bezpečnostní incident, a tak nebylo prioritou firmy to nějakým způsobem začít řešit. Na základní bezpečnostní pravidla je zaměstnanec upozorňován při přebírání počítače či e – mailové schránky, nicméně nemají ustálenou a koncepční podobu, mimo provozního řádu, kde je obecně popsáno chování pracovníků na pracovišti vč. uzamykání počítačů při odchodu apod. Tato pravidla však nejsou dodržována ani kontrolována.
Politika hesel	Politika hesel v organizaci neexistuje. Při předávání nové pracovní stanice (PC/notebook) je počítač vždy zabezpečen přihlašovacím jménem a heslem zvoleným zaměstnancem. Na žádném firemním počítači nesmí být obecný profil ani uživatelský účet nezabezpečený heslem. Využívání určitého typu hesel a jejich pravidelné obměňování ani pokročilejší způsoby autentizace se na firemní úrovni nevyžadují ani nekontrolují.
BYOD	Neexistují plošně platná pravidla o využívání soukromých zařízení pro pracovní účely (BYOD), záleží však na předmětu činnosti zaměstnance a na souhlasu nadřízeného.
Řízení přístupů	Řízení přístupů se řeší ad hoc, nemá jednotnou formu, ale existují nějaká nepsaná pravidla, např., že výplatní pásky vedení by neměly být přístupné všem uživatelům IS. V rámci NAS se řeší přidělování oprávnění, tj. kam má daný zaměstnanec v systému přístup, na žádost tak, že by měl vždy rozhodnout jeden ze tří ředitelů.
Klasifikace dat	Obecná klasifikace dat neexistuje. Zaměstnanci jsou však poučeni, která data jsou považována za citlivá, co je bankovní tajemství apod. při podpisu mlčenlivosti. Nicméně určitá forma klasifikace dat se začíná uplatňovat na sdíleném datovém úložišti, kde jsou mj. digitalizované personální složky zaměstnanců.

Citlivé informace	Nejcitlivějšími informacemi jsou pro podnik personální údaje, účetnictví a smlouvy. Je nutné zmínit, že oproti jiným firmám zde evidují, vzhledem k tomu, že se jedná o sociální podnik, celou řadu citlivých dokumentů obsahujících zdravotní dokumentaci zaměstnanců. Jedná se o různé skeny dokumentů, kde je popisován jejich hendikep, typ a výše invalidního důchodu (rozhodnutí o ID) a někdy i posudek, kde jsou již velmi detailní informace zdravotního charakteru. Tuto agendu je nutné vést kvůli pravidelným kontrolám z Úřadu práce, jelikož prokazují, že má společnost právo na čerpání příspěvků na chráněná pracovní místa.
Pravidla listinných dokumentů	Mezi základní dokumenty, které, byť okrajově, řeší pravidla listinných dokumentů patří GDPR směrnice, provozní řád, závazek mlčenlivosti a některé další dokumenty dle ČNB plynoucí ze spolupráce s bankovními subjekty. Tyto dokumenty se revidují přibližně jednou až třikrát ročně, nejčastěji vlivem nové legislativy či předpisů. Týkají se všech zaměstnanců i pracovníků na DPČ či DPP. Přímou odpovědnost za jejich dodržování má vždy manažer HR oddělení nebo administrativního týmu. Z pravidel lze zmínit např., že písemnosti obsahující osobní údaje mají být uchovávané v uzamykatelné skříni, je nastolená Clean Desk Policy atp., v praxi se však nedodržuje, ani nekontroluje. Velká část pravidel je však neformálního charakteru, jedná se o užívané postupy. Pravidelně probíhá kontrola všech personálních složek na případné nesrovnalosti. Důležité dokumenty jsou drženy v duální podobě – elektronicky i fyzicky. Společnost je ve vztahu ke GDPR v základní kategorii, nedochází zde k hromadnému zpracování dat.
Likvidace písemností	Neexistuje spisový řád ani skartační pořádek, tzn., že se ani nedávají skartační znaky, nicméně zástupci firmy připouští, že by to asi již měli začít řešit. Není také explicitně uvedené, které konkrétní dokumenty je třeba evidovat. Část zodpovědnosti ohledně likvidace je přenesena na externí mzdovou účetní. Na pracovišti je možné dokumenty skartovat, nejedná se však o certifikovanou skartovačku, ani není nijak zajištěn svoz skartovaných dokumentů.

Fyzická oblast

Do fyzické oblasti informační bezpečnosti spadá zejména (reálná) archivace a likvidace písemností a fyzický přístup k prostorám společnosti, resp. k jejich síťové architektuře – tj. k routerům, síťovým tiskárnám, switchům, Wi-Fi AP, NAS, ale i k síťové kabeláži).



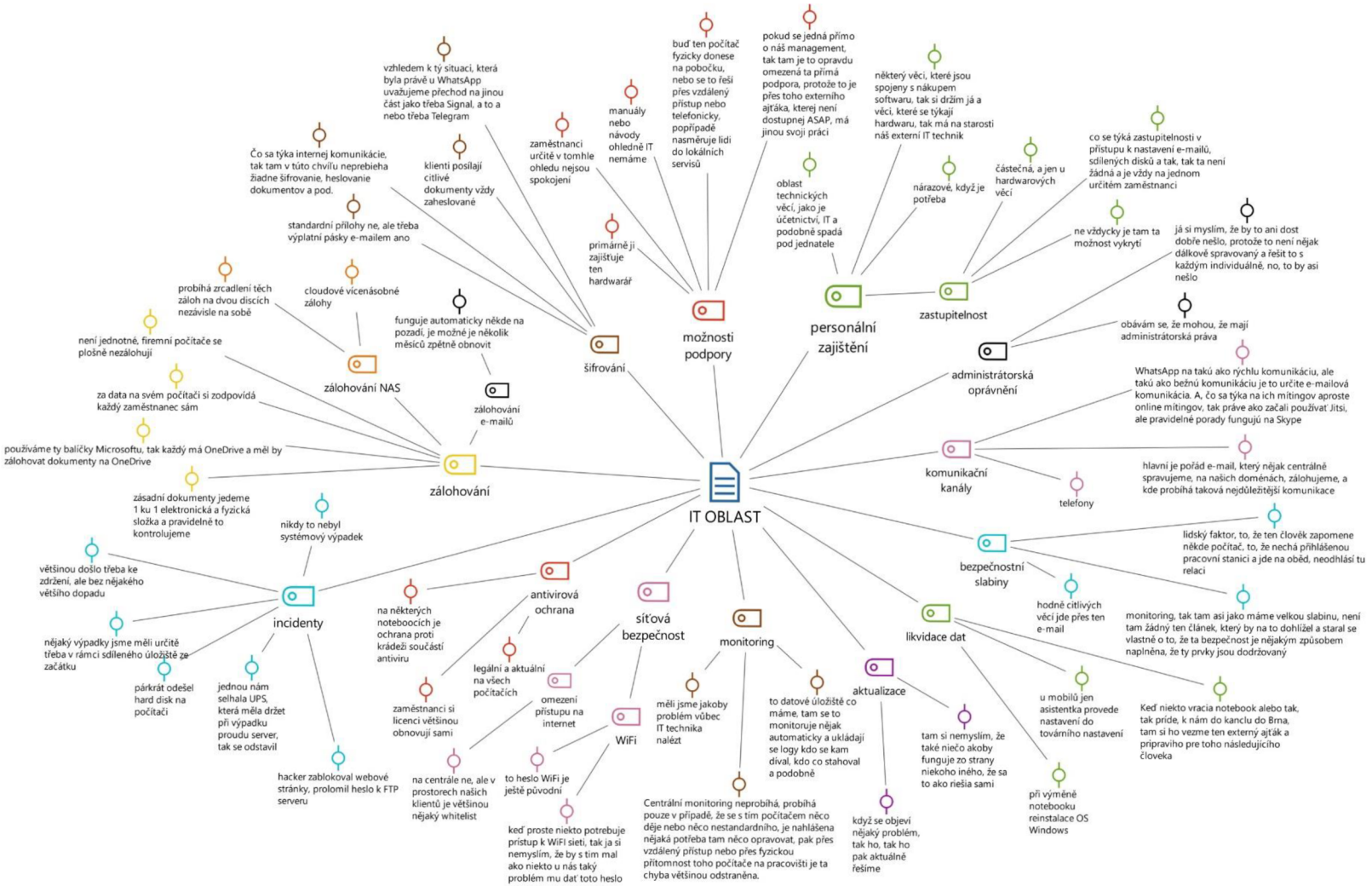
Obrázek č. 40: MAXMapa – fyzická oblast
(Zdroj: Novotný, 2022)

Tabulka č. 7: Shrnutí fyzické oblasti
(Zdroj: vlastní zpracování prostřednictvím MAXQDA)

Sklad	Externí archiv v suterénu firmy. Skladují se zde zejména historické dokumenty. Uzamčené, protipožární skříně, malá velikost.
Archivace v kanceláři	Archivace v kanceláři probíhá volně v policích. Není tam dostatek prostoru, což není komfortní pro zaměstnance. To je uváděno i jako jedna z příčin, proč zaměstnanci příliš nedodržují bezpečnostní pravidla ohledně písemností.
Zabezpečení prostor	Standardní zabezpečení, běžná uzamykatelná kancelář. Kancelář není vybavena EZS ani kamerovým systémem. Zabezpečení úměrné aktivům, nicméně existuje prostor pro navýšení bezpečnostních prvků.
Přístup k síťové architektuře	Přístup mají všichni zaměstnanci kanceláře. Síťová architektura není umístěná zvlášť ani speciálně fyzicky chráněná
Likvidace písemností	Likvidace je možná prostřednictvím necertifikované skartovačky, která je zaměstnancům k dispozici. Svoz senzitivního odpadu není zajištěn.

IT oblast

Oblast IT obsahuje jak pojmy týkající se personálního zajištění této agendy a zastupitelnosti pracovníků, tak možnosti podpory uživatelů IS, aktualizace software, monitoringu, síťové bezpečnosti, antivirové ochrany, (reálného) zálohování apod.



Obrázek č. 41: MAXMapa – IT oblast
(Zdroj: Novotný, 2022)

Tabulka č. 8: Shrnutí IT oblasti
(Zdroj: vlastní zpracování prostřednictvím MAXQDA)

Bezpečnostní slabiny	Vnímané bezpečnostní slabiny zahrnují lidský faktor (neukončování relací, neodhlašování počítačů, vzdálené připojení z domu), e – mail, absence monitoringu a kontroly.
Likvidace dat	Likvidace dat v případě odchodu pracovníka nebo změny jeho pracovního počítače je v gesci externího IT pracovníka, který však nemá žádnou certifikaci. Výmaz dat probíhá po předání počítače a vypořádání předávacích protokolů formou reinstalace operačního systému (Windows). U mobilních zařízení asistentka pouze provede nastavení do továrního nastavení.
Aktualizace	Aktualizace software na pracovních stanicích neprobíhá koordinovaně, ale je vždy na zaměstnancích. Spoléhá se na to, že vlivem automatických aktualizací bude aktualizování SW na uživatelích vynuceno, popř. proběhne automaticky. Případný problém se řeší pouze v případě, že ho zaměstnanec sám proaktivně nahlásí.
Monitoring	Centrální monitoring pracovních stanic neprobíhá. Pouze v případě, že je nahlášena potřeba něco opravovat, pak přes vzdálený přístup nebo přes fyzickou přítomnost toho počítače na pracovišti je chyba odstraněna. Na sdíleném datovém úložišti (NAS) probíhá automatický monitoring, navíc se ukládají logy všech událostí (kdo kam nahlížel, kdo co stahoval apod.)
Síťová bezpečnost	Povětšinou není problém se sdělováním hesla k firemní Wi-Fi síti. Není zřízen žádný guest účet s omezeným přístupem na intranet. Některá síťová zařízení jsou zabezpečena pouze výchozími hesly.
Wi-Fi	Heslo k Wi-Fi síti je cca 15místná kombinace alfanumerických a speciálních znaků, nicméně od přestěhování se do nové kanceláře nebylo změněno. Zaměstnanci běžně sdělují heslo k Wi-Fi síti návštěvám kanceláře (přesněji třeba partnerům, kteří o něj požádají).
Omezení přístupu na internet	Na centrále společnosti není žádné omezení přístupu na internet, neexistují žádné whitelisty, silný firewall apod.
Antivirová ochrana	Antivirová ochrana je legální a aktuální na všech počítačích. Případné licence pro obnovu nárokují zaměstnanci přímo u jednatele. Při nástupu zaměstnance obdrží pracovník pracovní stanici s přeinstalovaným OS (Windows) a předinstalovaným aktivovaným antivirem. Na vybraných noteboocích je součástí antiviru také ochrana proti krádeži.
Incidenty	Několikrát došlo ke ztrátě dat – při selhání HDD, poškození notebooku či vlivem nepoužívání zálohování. V minulosti došlo také k prolomení hesla k FTP serveru a napadení webových stránek. V nedávné době měla jedna zaměstnankyně "hacklý telefon". Jednou došlo vlivem špatné baterie k selhání UPS, což vedlo ke krátkodobému odstavení serveru. U sdíleného datového úložiště (NAS) dochází zřídka k výpadkům, jelikož stále není vyřešen provoz v případě výpadku el. sítě nebo internetového připojení.
Zálohování	Plošné zálohování pracovních stanic neprobíhá, nicméně vybraní zaměstnanci mají k dispozici cloudové řešení OneDrive, které je součástí balíčků Microsoft Office. U zásadních personálních dokumentů se praktikuje zálohování 1 :1 (elektronická a fyzická podoba), probíhá zde i pravidelná kontrola složek, jelikož jsou zde časté požadavky na kontrolu v rámci auditů z MPSV a ÚP. Obecně je politika nastavena tak, že každý zaměstnanec si za svěřená data odpovídá sám, nicméně prakticky vše je na bázi neformálních postupů.
Zálohování e – mailů	Zálohování e – mailů funguje automaticky, pravidelně, na externí cloud. Obnovit data je možné několik měsíců zpětně.
Zálohování NAS	Sdílené datové úložiště (NAS) je zálohované jednak formou mirroringu HDD (RAID 1), ale také na Synology C2 cloud.

Šifrování	Plošné šifrování příloh e – mailů neprobíhá, nicméně například distribuce výplatních pásek nebo citlivá komunikace s klienty obsahující citlivá data je šifrovaná. Při interní komunikaci se však žádná forma šifrování nevyužívá. Vzhledem k jistým problémům s aplikací WhatsApp uvažuje firma o přechodu například na Signal nebo Telegram.
Možnosti podpory	Možnosti IT podpory jsou minimální. Ohledně HW zajišťuje určitou omezenou přímou podporu externí IT pracovník, který buď problém fyzicky či vzdáleně vyřeší, nebo nasměřuje zaměstnance do lokálních servisů. Manuály nebo návody ohledně IT neexistují. Zaměstnanci se stávajícími možnostmi podpory nejsou spokojení, IT pracovník není často dosažitelný a řešení problémů trvá v řádu dnů.
Personální zajištění	Věci spojené s nákupem software si drží jednatel a záležitosti spjaté s hardware řeší externí IT pracovník nárazově.
Zastupitelnost	Zastupitelnost je pouze u hardware a to částečná. Ne vždy je tam možnost vykrytí. Zastupitelnost v nastavování e – mailů, sdíleného disku atp. není žádná.
Administrátorská oprávnění	Zaměstnanci mají plná administrátorská oprávnění na svých počítačích. Existuje názor, že by to nyní ani jinak řešit nešlo, vzhledem k tomu, že externí IT technik by neměl čas řešit problémy s každým individuálně.
Komunikační kanály	Hlavní je e – mail a telefon. Pro rychlou komunikaci slouží skupiny na WhatsApp. Online setkání se realizují nejčastěji na platformě Jitsi nebo Skype.

Poměrně konzistentní výpovědi účastníků rozhovorů svědčí o tom, že společnost si je určitých rizik ohledně informační bezpečnosti vědoma. Prakticky všichni dotazovaní pracovníci se shodují, že informační bezpečnost je oblastí, na kterou se firma nesoustředila, nicméně společně s překotným růstem podniku začíná být stávající situace ohledně ochrany informací v podniku neudržitelná. (Novotný, 2022) Níže je uveden doslovný přepis z rozhovorů:

„Je to v tom, že jsme vlastně, my jsme firma, která teďka jakoby došla k jako vlastně k velkému progresu, takže ten začátek určitě nebyla ta potřeba taková já nevím, dejme tomu, začínalo se na devíti zaměstnancích, pak bylo 20, 40 tak to je ještě takový počet, kdy to tolik neřešíte no, ale teď už jsme na stovce, na 130 prakticky a pak už, a ten přerod, ten progres byl prakticky jako během roku, byl veliký, takže spíš na to nebyla nějak jako potřeba, neměli jsme žádný incident, asi když to tak řeknu, takže ten čas vlastně ne jo, nebyla nebyla priorita té firmy toho nějak na to zaměřená.“ (U3, 2021)

„Ako firma proste momentálne ako rastieme, tzn. že som si istý, že sa to takéto niečo bude, bude skôr či neskôr musieť riešiť, ale nezachytil som doteraz, že by sa tak niečo akoby koncepčne riešilo.” (U2, 2021)

„Je asi logické, že proste, keď je firma mala, tak nejakým spôsobom tieto, alebo tieto veci začne riešiť až v momente, ako rastie a naberá zamestnancov, že v tomto prípade postupne ide, tzn. že, určite je namieste pripraviť si nejakú jednotnú bezpečnostnú

politiku, čo sa týka ochrany údajov. Momentálne teda nemám vedomosť o tom, že by takéto niečo fungovalo a určite je to ako do budúcna hrozba. Takže proste nejaké fakt nastavenie bezpečnostných pravidiel, o tom, o čem sme sa vlastne dneska celý den bavili, tak to je určite namieste, nejakých proste jednotných pravidiel pre celú firmu, ktoré by ako mali na starosti to, že by chránili tie osobné údaje firmy.“ (U2, 2021)

„Tam asi jako máme velkou slabinu si myslím, že tam není žádný jakoby ten článek, který by na to dohlížel a staral se vlastně o to, že ta bezpečnost je nějakým způsobem naplněna, že ty prvky jsou dodržovaný, no.“ (U4, 2021)

3.3.6 SWOT analýza IS

Níže jsou uvedeny identifikované silné a slabé stránky, příležitosti a hrozby týkající se současného stavu IS podniku vycházející ze souhrnu provedených analýz a empirického výzkumu.

Tabulka č. 9: SWOT analýza IS
(Zdroj: autor)

S (Silné stránky)	W (Slabé stránky)
Placený antivirový SW na všech PS Relativně moderní technika Motivovaní uživatelé IS takřka nepracuje s daty zákazníků Uživatelsky přívětivé UI Ochota investovat do IS/IT Nikde v systému neexistují sdílené uživatelské účty Doba odezvy IS	Absence bezpečnostních pravidel Náročnější adaptace uživatelů Informační gramotnost části uživatelů Chybějící informační strategie Absence školení v oblasti IS/IT Špatně nastavené pracovní postupy Chybějící metodika zálohování dat Špatné fyzické zabezpečení infrastruktury Nedostatečná technická podpora Absence uživatelské podpory Chybějící Disaster Recovery Plan
O (Příležitosti)	**T (Hrozby)**
Zavedení klasifikace dat Zavedení politiky hesel Zvýšení produktivity Stanovení bezpečnostních pravidel Zřízení funkce manažera IS/IT Zavedení nového IS CSRnet	Špatně nastav. proces odebírání přís. práv Kybernetický útok Ztráta a zneužití citlivých dat Zranitelnost podnikové sítě Kompromitace dat zaměstnancem Hrozba fyzického útoku, popř. živlu Plná administrátorská práva zaměstnanců Politika BYOD

4 VLASTNÍ NÁVRHY ŘEŠENÍ

Z analytické části, resp. provedených analýz vyplývá celá řada nedostatků, zejména v oblasti pravidel a bezpečnosti informačního systému. Některé návrhy a doporučení jsou obtížně finančně vyčíslitelné, jelikož značně závisí na rozsahu a kvalitě jejich provedení. Management podniku se také nemusí rozhodnou realizovat veškeré doporučované změny a navrhovaná opatření.

4.1 Souhrn doporučení z provedených analýz a empirického výzkumu

Níže jsou uvedena doporučení pro zlepšení podnikového informačního systému. Je využita kategorizace dle oblastí primárního výzkumu týkajícího se informační bezpečnosti, nicméně návrhy je také možné rozdělit například na doporučení a opatření technického rázu a doporučení a opatření organizačního charakteru či dále do dílčích logických celků.

4.1.1 Administrativní oblast

V podniku je nutné **vytvořit informační strategii**, tzn. stanovit cíle, kterých má být dosaženo a příslušné nástroje z oblasti IS vč. technického zabezpečení pro dosažení stanovených cílů. Podniková informační strategie je de facto návod, jak postupovat vč. harmonogramu, co pořídit, kdy a jak zavést vč. nástinu souvisejících kroků. Na přípravě informační strategie by se měl podílet jednatel společnosti, který má dosud tuto oblast v gesci a provozní ředitelka ve spolupráci s externím odborníkem.
S podnikovou informační strategií souvisí i **nutnost tvorby bezpečnostní strategie**, při jejíž tvorbě je nutné nejprve stanovit, jaká aktiva je třeba chránit, analyzovat rizika jim hrozící a stanovit opatření (jak technická, tak organizační) ke snížení či rovnou eliminaci těchto hrozeb. Bezpečnostní strategie pomáhá podniku vyvarovat se rizikových aktivit.

Pravidla a opatření ohledně informační bezpečnosti v podniku jsou na relativně nízké úrovni. Pravidla týkající se IT jsou spíše neformální. Je to způsobené mj. tím, že firma prošla za poslední rok velkým růstem, kdy se zněkolikanásobil počet zaměstnanců, nestal se žádný podstatný bezpečnostní incident, a tak nebylo prioritou firmy to

nějakým způsobem začít řešit. Je bezpodmínečně nutné **stanovit bezpečnostní pravidla IS**, které budou formulována například **v podobě směrnice či závazných pracovních postupů**. Tato směrnice či postupy musí definovat, jaká bezpečnostní pravidla musí pracovníci při výkonu své činnosti v rámci IS dodržovat. Nejedná se přitom pouze o pravidla ohledně IS, ale obecně především o nakládání s informacemi v podniku, chování na internetu nebo chování se na pracovišti či při odchodu z něho (vhodné je zavést např. pravidlo prázdného stolu a prázdné obrazovky), jednání v e – mailové korespondenci, nakládání s hesly apod. V podniku by měla být **uplatňována určitá bezpečnostní politika hesel**, kde bude specifikována frekvence změny (typicky alespoň jednou ročně), požadavky na tvorbu hesel (ideálně alespoň 8 alfanumerických a speciálních znaků) a na jeho bezpečné uložení. Není zdaleka dostačující mít tato pravidla pouze stanovená, není-li **dodržování pravidelně a systematicky kontrolováno a případné porušování sankcionováno**, přičemž je důležité zmínit, že pravidla musejí být dodržována všemi úrovněmi vedení. Aspekt řešení bezpečnostních pravidel by měl být dvojí – technický (tj. nastavení přístupových práv) a organizační (např. povinnost mlčenlivosti apod.). V každém případě je však nutné vždy jasně a konkrétně stanovit pravidla, kdo, kdy a s čím musí pracovat a s těmito pravidly seznámit pracovníky. Na **bezpečnostní pravidla** nestačí zaměstnance upozorňovat pouze při přebírání firemního počítače, ale je **nutné vypracovat jejich formalizovanou podobu a zaměstnance pravidelně školit**. Součástí formálních a písemných pravidel by bylo i vydefinování podmínek, které musejí pracovníci splnit pro využívání soukromých zařízení pro pracovní účely (BYOD).

Školení či jiné vzdělávání zaměstnanců ohledně informační bezpečnosti v podniku v žádné podobě v minulosti neprobíhalo a neprobíhá ani nyní. Na tento rok (2022) je však údajně naplánován budget na vzdělávání a počítá se s nějakou formou zvyšování IT dovedností zaměstnanců. Investice do vzdělávání zaměstnanců a propagace kultury bezpečnosti je nezbytným předpokladem funkčního systému ochrany informací podniku.

Bezpečnostní školení mohou být prováděna například externími subjekty, a to online s využitím gamifikace. Vzdělávací herní platforma CLASHING nabízí **interaktivní školení v oblasti informační a kybernetické bezpečnosti** za přibližně 300 Kč za uživatele na rok (ICT Pro, c2021). Alternativně je možné využít např. LMS Instructor,

který nabízí také online školení informační a kybernetické bezpečnosti. Jeden kurz stojí okolo 90 Kč bez DPH, v případě školení všech zaměstnanců je zde množstevní sleva a výsledná cena je okolo 80 Kč za uživatele za rok (INSTRUCTOR, c2022). Tento systém je poměrně oblíbený a užívaný mnohými podniky pro školení BOZP a PO. Školení by se v první vlně mělo týkat přibližně 30 zaměstnanců z řad managementu aktivně využívajících podnikový informační systém a stát by tudíž mělo 2700 Kč, resp. **9000 Kč (bez DPH)** v závislosti na vybrané variantě. Školení je možné případně rozšířit i o řadové zaměstnance, je však třeba zohlednit informační a bezpečnostní strategii při strategickém plánování. V budoucnu by roli školení a osvěty v oblasti (nejen) informační a kybernetické bezpečnosti mohl převzít nový systém CSRnet.

Bezpečnostní školení pracovníků by měla být **periodická**, je nutné jim **pravidelně připomínat bezpečnostní pravidla a zásady a upozorňovat je na hrozby** (nejen phishing a vishing), resp. na rizika plynoucí z nedodržování těchto zásad. Cílem je **vytváření tzv. bezpečnostního povědomí uživatelů** (SAE). Toto povědomí je nutné budovat postupně a kontinuálně, například interní osvětovou kampaní. Využít lze případně i služby tzv. etických hackerů, jichž využívají zejména velké firmy. Tyto společnosti nabízí zejména penetrační testy a simulace hrozeb sociálního inženýrství pro odhalení bezpečnostních nedostatků.

Oblast IT je také personálně podceněná, ve firmě chybí manažer IT, natožpak ISMS a z toho plyne mnohdy nejasné rozdělení rolí a odpovědnosti. V podniku je tedy nutné **zřídit funkci manažera pro informační systémy**. Je více než žádoucí vytvořit buď separátní pozici nebo pověřit někoho z vedení, aby systematicky řídil a dohlížel na tuto oblast, popř. spolupracoval s externím konzultantem. Je samozřejmě otázkou, nakolik je v podniku prostor pro takovéhoto zaměstnance na plný úvazek, byť by třeba již nebylo nutné využívat služby externích IT pracovníků. **Ideálním stavem by bylo zřídit také funkci manažera informační bezpečnosti**, resp. alespoň pověřit určitého pracovníka jejím řízením.

Úroveň uživatelské podpory je nedostatečná. Možnosti přímé IT podpory uživatelů IS jsou omezené, což je primárně způsobeno tím, že IT technik je externista a jeho zastupitelnost je minimální. V oblasti IS/IT je tedy nutné **zajistit alternativu ke klíčovým pracovníkům**. Zastupitelnost klíčových pracovníků je zcela esenciální,

jelikož jejich nedostupnost např. z důvodu nemoci, může mít pro podnik vážné dopady a musí být tedy připraveno záložní řešení např. v podobě smluvního vztahu s dodatečným externím pracovníkem. Je třeba zajistit dostupnost podpory jak pasivní, např. ve formě **uživatelských příruček či manuálů**, tak aktivní, tj. **možnost kontaktování helpdesku**, resp. pozice, kam se mohou uživatelé obracet s problémy IS/IT. Pro pracovníky se systémem musí být veškeré potřebné informace snadno dostupné, a především přehledné a srozumitelné. Absence pasivní uživatelské podpory klade zvýšené požadavky na, obvykle nákladnější, podporu aktivní. Pokud pracovníci sami hlásí problémy s IS/IT, je vhodné jednotlivým hlášením přiřadit různé stupně priority lišící se požadovanou dobou na reakci a vyřešení problému tak, aby řešení nebylo příliš nákladné, ale zároveň, aby se minimalizoval vliv problému na produktivitu zaměstnance, resp. chod pracoviště. Chybějící uživatelská podpora je paradoxně povětšinou závažnější než chybějící technická podpora, jelikož závady na technice nejsou obvykle tak četné jak chyby uživatelů PIS. Informovaný uživatel, který nemusí potřebné informace složitě hledat je pochopitelně produktivnější a má menší chybovost. Nemělo by se proto opomíjet **proškolení nových pracovníků v užívání informačního systému**. Zvláště pro nové zaměstnance může být zapracování do IS vzhledem k absenci jakýchkoliv návodů minimálně zmatečné. Ostatně, i stávající zaměstnanci nejsou se stávajícími možnostmi IT podpory spokojení a vyřešení problémů trvá často i v řádu dnů. K systematickému zlepšování systému, popř. jeho inovování je také nutné získávání zpětné vazby. Za tímto účelem je dobré **zřídit kontaktní místo pro hlášení závad a vznášení požadavků týkajících se IS**. Kontaktní osoba pak předává požadavky dál odpovědným osobám – např. technikům či vedení.

V oblasti procesního řízení je podstatné **stanovit přesná pravidla, jak jsou dané činnosti vykonávány**. Je tedy nutný **vznik procesní dokumentace**. Tato pravidla mohou mít formu závazných pracovních postupů či směrnic, je však nutné vždy jasně specifikovat odpovědnost pracovníků tak, aby nedocházelo k prodlením a možným ztrátám. V oblasti IS by pravidla měla zejména odpovídat na otázky kdo, kdy, jakou činnost provádí a co je povinen nebo co naopak s informačním systémem dělat nesmí. Směrnice by také měla obsahovat **návod, jak postupovat v případě potíží** – na koho se obrátit apod. Je nutné **zlepšit proces managementu přístupových práv do systémů, zvláště pak jejich odebírání**. Potřebné jsou systematické kontroly aktuálnosti – zda

veškeré účty a jejich oprávnění odpovídají realitě. Požadavek na ukončení přístupových práv zaměstnance při jeho odchodu, popř. změně pracovního zařazení, musí pověřený pracovník vypořádat co nejdříve. Obdobně, byť s o něco nižší prioritou, musí správně fungovat proces zavedení práv nového pracovníka při jeho nástupu nebo změně pracovního zařazení. Tuto problematiku neovlivňuje ani tak informační systém, jako špatně nastavené procesy.

Podnik musí vyřešit **klasifikaci dat**, jelikož dosud neexistuje. Tato klasifikace musí stanovovat, které dokumenty musí být zničeny a jakým způsobem. Zaměstnanci jsou však poučeni, která data jsou považována za citlivá, co je bankovní tajemství apod. při podpisu mlčenlivosti. Nicméně určitá forma klasifikace dat se začíná uplatňovat na sdíleném datovém úložišti, kde jsou mj. digitalizované personální složky zaměstnanců. Definice konkrétních dokumentů a klasifikace dat by měla být součástí nově vzniknuvších pravidel informační bezpečnosti. Obdobně jako klasifikace dat, i řízení přístupů se řeší ad hoc a existují pouze určitá nepsaná pravidla. Přístupy je nutné, ostatně jakou celou bezpečnostní politiku podniku, řešit koncepčně a plošně, k čemuž je nutné mít jednoznačně a písemně definované podmínky. Co se týká listinných dokumentů, ve společnosti neexistuje spisový řád, a tudíž ani skartační pořádek, nicméně zástupci firmy připouští, že by to již měli začít řešit. De iure se v podniku praktikuje Clean Desk Policy, de facto se však nedodržuje, ani nekontroluje, což plyne mj. z toho, že velká část pravidel je silně neformálního charakteru a jedná se o víceméně o užívané postupy. To se týká i **pravidel skartace**, jelikož je používána skartovačka, která **není certifikována a není zajištěn svoz** citlivého odpadu. Nejsou-li v podniku explicitně formulované předpisy ohledně bezpečnosti a pokud už existují, nejsou často kontrolovány a nelze se tudíž podivovat nad jejich nedodržováním.

V souvislosti s pravidly týkajících se nakládání s daty, resp. s likvidací citlivých dat je v podniku nutné **určit osobu odpovědnou za jejich likvidaci**, případně více osob dle různých typů datových nosičů a zabránit tak úniku informací z firmy. Likvidovat je třeba nejen nepotřebná data uložená v elektronické podobě na datových nosičích, ale běžně dochází také k likvidaci listinných dokumentů, a to povětšinou skartací. Digitální média se likvidují buď fyzickým zničením (rozdrcení apod.) nebo vícenásobným přepisem pomocí speciálního softwaru.

Nejcitlivějšími informacemi jsou pro podnik personální údaje, účetnictví a smlouvy, naopak s daty o zákaznících se téměř nepracuje. Je nutné připomenout, že oproti jiným podnikům zde evidují, vzhledem k tomu, že se jedná o sociální podnik, celou řadu dokumentů obsahujících podrobnou zdravotní dokumentaci zaměstnanců. Tyto personální složky by tedy měly mít nejvyšší stupeň zabezpečení proti úniku dat.

Další nezbytným doporučením je **vytvoření metodiky zálohování** podnikových dat. Scénář zálohování je potřebné mít zejména v případě vlastní hardwarové infrastruktury, na níž je IS provozován, ale i když je část dat u poskytovatele cloudových služeb, je nutné se aktivně zajímat o to, jakým způsobem a s jakou periodicitou jsou data zálohována. Zálohovat je nutné i data na pracovních počítačích, obsahují-li důležité informace. Vždy je nutné mít na paměti, že zálohovaná data je nutné chránit stejně, jako originální data – tj. například flash disk se zálohou účetnictví nenechávat volně na stole nebo zálohy kriticky důležitých systémů neumísťovat na veřejná cloudová úložiště. Součástí problematiky zálohování by měl být i **vypracovaný postup obnovy dat**, který je obecně součástí směrnice nebo postupu pro řešení havarijních situací. Společnost tento plán (Disaster Recovery) zpracovaný nemá, nicméně existuje vypracovaný BCP (Business Continuity Plan), který je společnost povinna držet pro svého zákazníka z bankovního odvětví. Neexistují však žádné postupy, např. co dělat při výpadku NAS – proto by se **zpracováním alespoň jednoduchého dokumentu popisujícího pravděpodobné krizové scénáře v oblasti IS/IT** neměli otálet. Po havárii je obvykle důležité postupovat rychle a pracovníci IT jsou často značně pod tlakem. Je nutné ihned vědět jaké zálohy se mají odkud obnovovat, stejně jaké je pořadí obnovy systémů – jaké jsou priority. K dispozici musí být přístupové údaje, aby byla řešena zastupitelnost klíčových pracovníků. Cílem pochopitelně je v co nejkratším čase obnovit funkčnost IS. Tyto postupy by měly obsahovat návod na řešení možných problémů, a to v detailu potřebném nutném pro jeho realizaci v podmínkách daného IS podniku. Zálohy dat je třeba udržovat aktuální, stejně jako mít ideálně **připraveny záložní technické prostředky pro klíčové části systému**, což je zvlášť akcentováno v případě, kdy informační systémy využívají pro svůj chod vlastní infrastrukturu podniku, což je případ NAS Synology.

4.1.2 Fyzická oblast

Je nutné **zajistit fyzickou ochranu techniky**, a to jednak před fyzickým útočníkem, nebo působením živlu, zejména požáru. Fyzický přístup k síťové architektuře **není nijak zvlášť chráněný** a např. připojit zařízení do interní sítě LAN mimo pracovní dobu lze bez jakýchkoliv potíží. Řešením je **omezit přístup k síťovým zařízením**, minimálně pomocí uzamykatelné odvětrávané skříně **a posílit zabezpečení kanceláře**, v níž jsou tato zařízení uložena. Obecné zabezpečení prostor je víceméně standardní, kancelář, ani dům, jehož je součástí není vybavena bezpečnostním zařízením ani kamerovým systémem, nicméně jednatel společnosti uvažuje o **pořízení EZS**. Pokud není možné, vzhledem k dispozičním možnostem, důležitou síťovou architekturu například stavebně oddělit, je **důležité alespoň zvýšit ochranu portů** (více viz. IT oblast).

V souvislosti se zabezpečím techniky je nutné **zvážit nutnost připojování externích médií k počítačům pracovníků**. Záleží samozřejmě na důvěrnosti dat obsažených v daném konkrétním zařízení, nicméně současná situace zvyšuje riziko infikace počítačů škodlivými soubory. Pokud se podnik rozhodne nějakou formu omezení vyžadovat, mělo by to být nejen zakázáno organizačním předpisem, ale také podchyceno odpovídajícím technickým nastavením.

Pomineme-li externí mzdovou účetní, společnost archivuje listinné dokumenty primárně dvojím způsobem. Jednak přímo v kanceláři společnosti, ale také v externím suterénním skladu, kde se skladují zejména historické, nepoužívané, dokumenty. Tento sklad je sice malý, ale protipožární a samostatně uzamykatelný. Poněkud **problematické je dlouhodobé skladování písemností volně v kanceláři**, což je zřejmě dáno opět především tamními prostorovými dispozicemi, které jsou omezené. Minimálním a relativně málo nákladným opatřením by bylo pořídit na tyto dokumenty **uzamykatelné skříně a nastavit určité postupy přístupu k nim**, zejména v době, kdy není kancelář používána a chodí tam např. uklízečky. Likvidace listinných dokumentů je možná prostřednictvím necertifikované skartovačky, která je zaměstnancům k dispozici, nicméně v praxi se příliš často nevyužívá.

4.1.3 IT oblast

Neexistuje žádná koncepce bezpečnosti či používání IT techniky, existují pouze obecná pravidla, která jsou z části zahrnuta v provozním řádu podniku, avšak k jejich kontrolování a ani vymáhání v praxi nedochází, nedojde-li k nějakému problému. Případný problém se řeší pouze v případě, že ho zaměstnanec sám proaktivně nahlásí, nejsou stanovené žádné postupy ani řešení různých situací týkajících se IT/IS. Stejně tak **aktualizace software na pracovních stanicích neprobíhá koordinovaně**, ale je vždy ponechána na zaměstnancích. Spoléhá se na to, že vlivem automatických aktualizací bude aktualizování SW na uživatelích vynuceno, popř., že proběhne automaticky. Centrální monitoring pracovních stanic taktéž neprobíhá. Na sdíleném datovém úložišti (NAS) však automatický monitoring probíhá, a navíc se ukládají logy všech událostí (kdo se kam díval, kdo co stahoval apod.), avšak s těmito daty se dále nijak nenakládá, slouží pouze k řešení případného problému (tj. **není zde systém, který by automaticky upozornil na nestandardní aktivitu**). Součástí nově nastavované bezpečnostní politiky musí být kromě zmíněného monitoringu zařízení řešena i otázka aktualizací a stanoveny zodpovědnosti pracovníků za jejich kontrolování, jelikož zastaralý systém je potenciálním bezpečnostním rizikem.

Heslo k síti Wi-Fi je sice „bezpečná“ dlouhá kombinace znaků, avšak **nebylo změněno více jak rok a půl a způsob jeho fyzického uložení je taktéž zcela nevyhovující**. Je důležité **vytvořit oddělenou síť pro návštěvníky**, popř. přístupu cizích osob do podnikové sítě zcela zamezit, což v době relativně levných mobilních dat povětšinou nepředstavuje značný problém. Bude-li společnost pokračovat v umožňování přístupu do zabezpečené sítě třetím osobám, měl by být minimálně zřízen tzv. **guest účet s defaultně omezeným přístupem k firemnímu intranetu**. Současně by měl probíhat **monitoring zařízení připojených do sítě LAN**. Některá zařízení jsou navíc zabezpečena pouze výchozími hesly a je tedy nutné tato **síťová zařízení zabezpečit odpovídajícím způsobem**. S tím souvisí i fakt, že firemní síť není chráněna žádným firewallem. Vnitropodniková **síť musí být firewallem zabezpečena**, a to nejen na koncových stanicích, ale také na ostatních síťových prvcích, jakou jsou například routery nebo switche.

Legální placená antivirová ochrana pracovních stanic je nainstalována na všech zařízeních zaměstnavatele, zlepšit by však chtělo systém aktualizování a případně **rozšířit modul ochrany proti krádeži i na ostatní přenosná zařízení, nejen na notebooky ředitelů.** U sdíleného datového úložiště (NAS) stále **chybí záložní zdroj (UPS)**, zálohování jeho dat je však vyřešeno dostatečně (mirroring a cloud). A ačkoliv je zálohování např. NAS na relativně dobré úrovni, bylo by vhodné **přistupovat k problematice zálohování koncepčně** a vypracovat postupy zahrnující všechna zařízení, kde jsou uchovávána důležitá a citlivá data. **Vzhledem k neexistující politice zálohování nedochází k plošnému zálohování pracovních stanic**, byť je zde možnost zálohy důležitých dat do cloudu (OneDrive pro firmy) popř. na NAS. Interní komunikace není šifrovaná a vzhledem k neexistenci politiky hesel by společnost měla uvažovat o **šifrování citlivých dat i v rámci interní komunikace mezi pobočkami**, nebo využívat NAS jako úložiště dat a odesílat pouze veřejný odkaz do zabezpečené složky.

Co je určitě třeba změnit je **nastavení plného administrátorského přístupu na PS zaměstnanců**. Je třeba zvážit nutnost instalace programů na počítače samotnými pracovníky, jelikož toto může způsobit narušení bezpečnosti nejen koncové pracovní stanice (předmětného počítače), ale potenciálně i celé sítě. Je také nutné je upozornit na možné právní konsekvence v případě instalace ilegálního softwaru na pracovní počítač zaměstnancem. Paušálně toto pracovníkům povolovat lze považovat za hazard. Zazněl však názor, že vzhledem k tomu, že externí IT technik by neměl čas instalace programů řešit s každým individuálně, jinak to ani nešlo, což opět připomíná nutnost vlastního IT pracovníka. Pracovníky vnímané bezpečnostní slabiny zahrnují především **lidský faktor** (konkrétně např. neukončování relací, neodhlašování počítačů, vzdálené připojování z domu přes VPN), e – maily, absenci monitoringu a jakékoliv kontroly. Jedná se o oblasti, z nichž většinu z nich lze řídit prostřednictvím kvalitně nastavené bezpečnostní politiky podniku (viz. Administrativní oblast).

4.2 Implementace systému CSRnet

Stěžejní navrhovanou změnou je implementace nového IS – aplikace CSRnet zmíněné výše. Tento zaměstnanecký podnikový portál bude sloužit pro jejich školení, testování a realizaci průzkumů, ale také jako systém distribuce značné části benefitů. Úspěšně

zvládnutá implementace přinese mj. zásadní zefektivnění některý procesů, a především úsporu času, zvláště v oblasti distribuce benefitů. Součástí plánu implementace je také Lewinův model popisující vlastní změnu, časová analýza vč. síťového grafu PERT a analýza rizika spjatého s procesem implementace.

4.2.1 Lewinův model

Dle Lewinova modelu řízení změny by změna v organizaci měla probíhat ve třech fázích – fázi rozmrazení, fázi přechodu a aplikace změny a ve fázi zmrazení.

4.2.1.1 Fáze rozmrazení

Ve fázi rozmrazení jsou síly inicializující proces změny, resp. stávající pravidla, zvyklosti a způsoby myšlení rozmrazeny, tj. rozvolněny. Na počátku fáze rozmrazení musí představitelé společnosti rozhodnout o samotném zavedení informačního systému, resp. nové aplikace. Předně je třeba vymezit prostředky nutné ke změně a poté se může zahájit proces přípravy implementace. Implementaci bude mít na starost externí IT specialista společně s jednatelem společnosti, který má dosud oblast IS/IT v gesci (připomínám, že v podniku chybí manažer IS/IT) a to ve spolupráci s dodavatelem systému (jedná se o činnost A). V rámci této fáze musí proběhnout také vytvoření dokumentace pro nový IS, načež se vytvoří kompletní plán zavedení.

4.2.1.2 Analýza silového pole

Škála byla stanovena od +1 do +5 pro změnu dle významnosti (1 - nejméně významná, 5 - nejvíce významná) a vice versa.

Tabulka č. 10: Síly pro změnu
(Zdroj: autor)

Síla pro změnu	Hodnota síly
Zvýšení efektivity práce	+5
Vlastník podniku	+5
Management firmy	+4
Personalistka	+3
Menší roztříštěnost používaných aplikací	+2
Mzdová účetní	+1
SOUČET SIL	**+20**

Tabulka č. 11: Síly proti změně
(Zdroj: autor)

Síla proti změně	Hodnota síly
Minoritní část zaměstnanců	-4
Náklady na školení	-3
IT technik – helpdesk	-2
Sociální pracovnice (psychosoc. podpora)	-1
SOUČET SIL	**-10**

Hlavní silou pro změnu by nemělo být pouhé pořízení relativně nákladného systému a nutnost jeho upotřebení. Pro změnu působí zejména tlak vlastníka firmy a jejího vedení plynoucí z potřeby zefektivnění určitých procesů. Pro zavedení je také mzdová účetní a personalistka, kterým IS usnadní práci (zejména administrativní činnost). Proti změně se naopak může stavět menší část zaměstnanců, kterým vyhovuje současný stav a u nichž se nepředpokládá, že by tento systém aktivně využívali. Jedná se například o lidi, kteří neradi pracují s počítačem a internetem, jsou obecně k technice konzervativnější a ve zběhlých procesech setrvačnější.

Tito lidé obecně hůře snášejí změny a jejich zapojení do používání je značně omezené, což může zlepšit kvalitní zaškolení, popř. určitá adopční kampaň. Implementace informačního systému do tolika oblastí ve firmě bude také znamenat více práce pro podnikového IT pracovníka (externistu) a sociální pracovnici, která v současnosti zajišťuje podporu zaměstnancům, byť primárně v oblasti mimopracovních záležitostí. Na základě výsledků analýzy silového pole lze konstatovat, že více silnějších faktorů působí pro změnu (výsledná suma je kladná a to +10), tudíž změnu je možné realizovat.

4.2.1.3 Nositel změny

Agentem změny je externí IT pracovník, jednatel společnosti a pracovník dodavatele systému. Sponzorem změny jsou představitelé společnosti, tj. vlastník firmy a její vedení. Advokátem změny je pak značná část zaměstnanců i manažerů, zejména personalistka a mzdová účetní.

4.2.1.4 Intervenční strategie

Identifikace intervenčních oblastí, je důležitým krokem v řízení změn. Níže uvedené jednotlivé intervenční oblasti popisují vztah ke společnosti a k implementaci informačního systému. Intervenční oblasti plánované firemní změny můžeme rozdělit na lidské zdroje a jejich řízení, organizační strukturu firmy, technologii firmy (z

hlediska produktu, služby a dalších doplňkových služeb) a komunikační a organizační toky a procesy firmy. V oblasti **lidských zdrojů a jejich řízení** nedojde ve společnosti k výraznějším personálním změnám, dojde však k jejich efektivnějšímu řízení tím, že se transformuje značná část agendy do online prostředí (e – learning, dotazníky, výběr benefitů). Po nasazení aplikace do provozu veškeré předmětné aktivity řízeny výhradně s využitím daného informačního systému. **Organizační struktura** společnosti nebude implementací aplikace CSRnet prakticky nijak dotčena a není zde předpoklad, že by došlo např. k propuštění některý zaměstnanců zodpovědných za vyřizování benefitů, jelikož tyto činnosti netvoří většinu náplně jejich pracovní činnosti. Ve společnosti dojde implementací ke změně v některých **technologiích**. Co se hardwaru týče, společnost nemusí dovybavovat žádné pracoviště. Aplikace bude hostovaná na serverech externího poskytovatele a pro přístup k ní postačí běžný internetový prohlížeč na běžném koncovém zařízení (počítači či mobilním zařízení). Nový IS však bude pro svoji plnou funkčnost vyžadovat napojení na mzdový software (viz. nedávné požadavky), aby mohlo docházet k automatizovanému rozesílání výplatních pásek do uživatelských profilů jednotlivých zaměstnanců. **Komunikační tok** se rozšíří o nový kanál – systém CSRnet totiž může částečně fungovat jako určitá sociální platforma, a tak usnadnit komunikaci mezi jednotlivými zaměstnanci stejně tak jako mezi celými týmy či pobočkami. Podnik si od tohoto slibuje posílení firemní kultury a zvýšení sounáležitosti mezi zaměstnanci z různých poboček a měst. K dispozici může být i forma chatu, ta však klade vyšší nároky na hosting, na kterém je aplikace provozována. Prostřednictvím CSRnetu se také digitalizují některé procesy, například distribuce benefitů už nebude probíhat skrze telefon či e – mailovou korespondenci, a počítá se i s interní podnikovou „wikipedií“, určitou znalostní bází, kde budou přístupné veškeré dokumenty s postupy, informacemi a návody, které mohou zaměstnanci během výkonu činnosti potřebovat.

4.2.1.5 Fáze přechodu a aplikace změny

Samotná realizace změny se skládá z celého sledu činností, z nichž nejdůležitější jsou uvedené v tabulce níže. Během této fáze je nutné kontrolovat reálný průběh oproti plánu a analyzovat odchylky. Před ostrým spuštěním, resp. nasazením přejde informační systém do fáze testování, během kterého dojde k odhalení možných problémů, které bude potřeba před ostrým startem opravit. Výsledkem této fáze by tedy měla být

korektně fungující aplikace plnící stanovené požadavky v běžném provozu. Stanovené dílčí cíle by přitom měly být SMART (tedy specifické, měřitelné, přiřaditelné, realistické a časově ohraničené). Každý milník projektu by měl být také binární – tedy buď dokončený či nedokončený. Tato opatření pomohou projekt řídit, zvláště v organizaci, která prošla prudkým rozvojem a některé činnosti v oblasti řízení projektů a procesů jsou stále značně chaotické. Z hlediska strategie zavádění IS je jedná o strategii postupnou, tj. odebírání částí starého systému a jejich nahrazování částmi systému nového. Uvažovat by šlo i o pilotním provozu, což je nicméně poměrně problematické řešení a je zde vyšší riziko vzniku chaosu vzhledem k tomu, že značná část procesů je řízena direktivně z brněnské centrály.

Tabulka č. 12: Tabulka činností
(Zdroj: autor)

Označení činnosti	Popis činnosti
A	Schválení rozpočtu, definování zodpovědných osob a vymezení kompetencí
B	Konfigurace esenciálního nastavení administrátorem
C	Spuštění testovací demo verze
D	Tvorba nastavení gamifikačního systému
E	Integrace se systémem na zpracovaní mezd
F	Tvorba benefitů způsobilých pro distribuci e – shopem
G	Nahrání obsahu e – learningu a dotazníků
H	Příprava testovacího prostředí (na betatest)
I	Betatest na vybraných zaměstnancích (funkcionalita; UI a výsledný UX)
J	Úprava IS dle výsledků betatestu, odstranění chyb
K	Vyhotovení seznamu uživatelů
L	Definování pravidel používání IS, tvorba interních směrnic
M	Tvorba uživatelské dokumentace
N	Migrace mzdových dat do IS
O	Nastavení přístupových práv
P	Zaškolení koncových uživatelů – manažeři
Q	Zaškolení koncových uživatelů – zaměstnanci
R	Příprava strategie spuštění
S	Aktivace uživatelských účtů
T	Bezpečná distribuce přihlašovacích údajů mezi pracovníky
U	Zřízení helpdesku pro zaměstnance v souvislosti se spuštěním IS
V	Oficiální spuštění IS
W	Vyhodnocení úspěšnosti spuštění IS

4.2.1.6 Fáze zmrazení

Výstupem fáze zmrazení je odsouhlasení stavu změny, tj. implementované aplikace CSRnet a následné „zamrazení“ stavu. Je přitom důležité sledovat, zda došlo k naplnění očekávání a stanovených cílů (činnost W), což v tomto případě mimo jiné znamená najít vhodné metriky, jak hodnotit efektivnost informačního systému. Výsledná efektivnost také nakonec závisí na lidském faktoru více, než by se mohlo zdát a je nutné dbát důrazu na přívětivé uživatelské prostředí (UI) přístupné pro všechny zaměstnance včetně těch s horším zrakem. Společnost by se měla poučit ze selhání implementačních snah u předcházející aplikace. Důkladné musí být také proškolení zaměstnanců, resp. uživatelů IS tak, aby jeho používání bylo pro ně intuitivní a pohodlné. V případě, že by uživatelé systém nepoužívali, resp. byly by do jeho používaní nuceni ze strany vedení a tento systém by neplnil svoji určenou roli, jednalo by se o selhání projektu.

4.2.2 Analýza rizik

Níže provedená analýza rizik slouží primárně k ohodnocení pravděpodobnosti a dopadů (tudíž k ohodnocení výsledných hodnot) vybraných rizik na projekt implementace aplikace CSRnet. Pro účely této práce byla zvolena skórovací metoda využívající odhady pravděpodobnosti a dopadu. Zvolené měřítko je 1 až 5 , přičemž hodnota jedna znamená minimální pravděpodobnost či téměř neznatelný dopad a vice versa. Maximální možná hodnota výsledného rizika, tedy součin pravděpodobnosti a dopadu, je tudíž 25.

Tabulka č. 13: Hodnocení pravděpodobnosti výskytu rizika
(Zdroj: autor)

Pravděpodobnost	Hodnota
Velmi nízká, téměř nemožná	1
Nízká, výjimečně možná	2
Střední, možná	3
Vysoká	4
Velmi vysoká, hraničící s jistotou	5

Tabulka č. 14: Hodnocení dopadu rizika
(Zdroj: autor)

Dopad	Hodnota
Velmi malý, téměř neznatelný	1
Malý	2
Střední, významný	3
Vysoký	4
Velmi velký, kritický	5

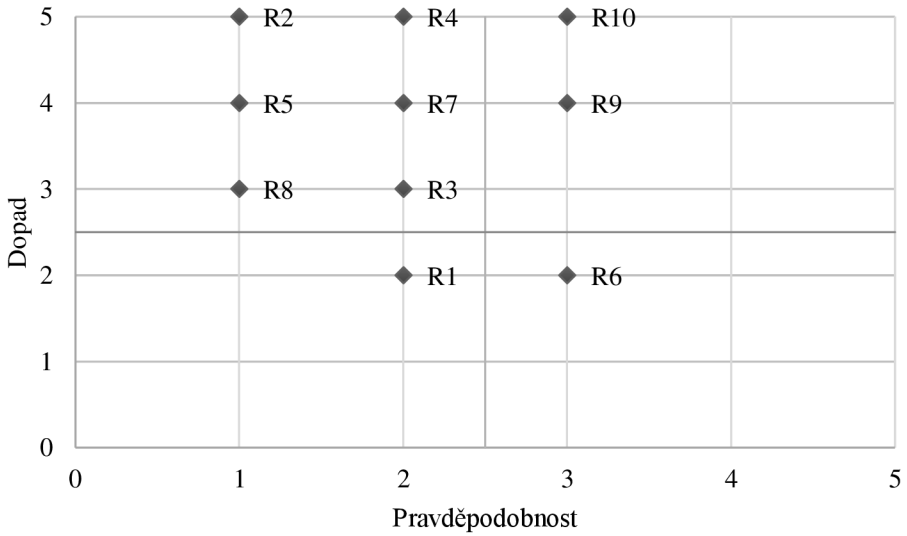
Tabulka č. 15: Hodnocení významnosti rizika
(Zdroj: autor)

Významnost	Popis	Hodnota
Zanedbatelná	Málo významné riziko neohrožující projekt, není nutné řešení	1-7
Znatelná	Významné riziko ohrožující projekt, je nutné včasné řešení	8-12
Značná	Kritické riziko s význam. dopadem na projekt, nutné okamžité řešení	13-25

Tabulka č. 16: Analýza rizik
(Zdroj: autor)

Číslo rizika	Hrozba	Scénář	Pravděpodobnost	Dopad	Hodnota rizika
R1	Zdržení při integraci mzdového systému	Současný ext. mzdový IS nemusí ihned spolupracovat s novým systémem a modifikace propojení může nabrat zpoždění, což zapříčiní, že tento modul nebude v novém systému fungovat	2	2	**4**
R2	Ztráta dat při transportu databází	Při transferu dat z databází dojde ke ztrátě či nevratnému přepisu některých údajů	1	5	**5**
R3	Systém má po spuštění prodlevy	IS se bude uživatelům načítat dlouho, což komplikuje jejich práci	2	3	**6**
R4	Systém má po spuštění výpadky	IS bude mít výpadky - tzn. někdy se vůbec nenačte a zadaná data se neuloží	2	5	**10**
R5	E-shop s benefity je fin. neudržitelný	Nastavení zaměstnaneckých benefitů v interním e-shopu je špatné	1	4	**4**
R6	Lidé si stěžují na gamifikační systém	Gamifikační prvky nebudou přinášet očekávaný efekt, zaměstnanci nebudou s nastaveným systémem spokojeni	3	2	**6**
R7	Uživatelé systém příliš nevyužívají	Uživatelé nevidí v IS oporu, tak se snaží pro dané procesy využívat jiná řešení	1	5	**5**
R8	Odchod technika zodpov. za provoz	Administrátor IS ukončí svůj pracovní poměr ve firmě	2	4	**8**
R9	Zaměstnanci neví, jak se systémem pracovat	Uživatelé IS tápou v IS a neorientují se, jejich práce je neefektivní	3	4	**12**
R10	Nastane vážný bezpečnostní incident	Např. následkem kyberútoku či selhání lidského faktoru dojde k narušení integrity a ke kompromitaci uživatelských dat	3	5	**15**

Nejvyšší výslednou hodnotu dopadu má riziko R10 (tj. že nastane vážný bezpečnostní incident) a to konkrétně 15, nejnižší naopak riziko R1 (tj. zdržení při integraci mzdového systému), pouhé 4.



Graf č. 3: Matice rizik před opatřením
(Zdroj: autor)

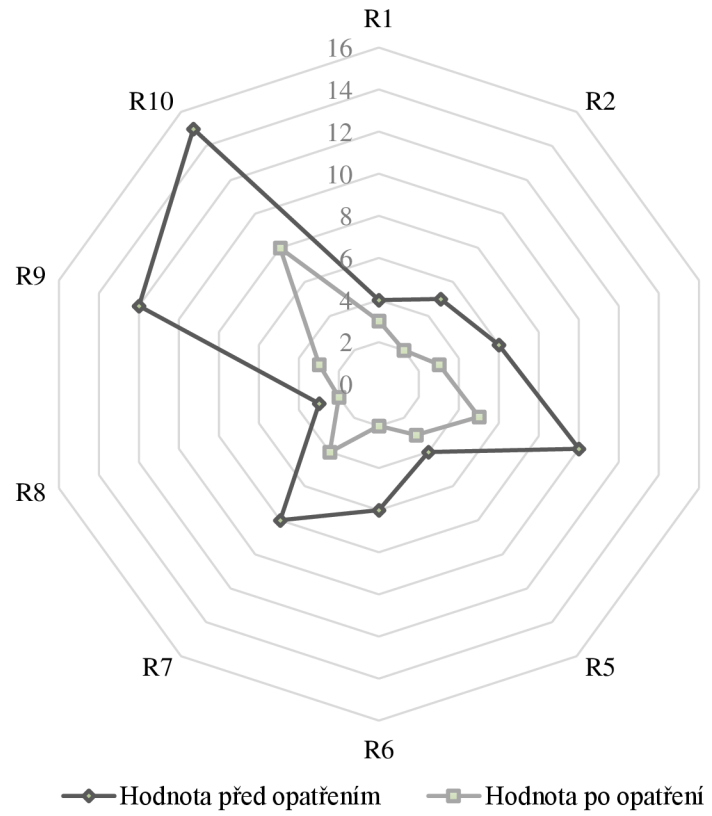
Z mapy, resp. matice rizik před opatřením je patrné, že nejvíce identifikovaných rizik spadá do kvadrantu vysokého dopadu a nízké pravděpodobnosti vzniku.

Tabulka č. 17: Analýza rizik po navrhovaných opatřeních
(Zdroj: autor)

Číslo rizika	Hrozba	Návrh opatření	Nová pravděpodobnost	Nový dopad	Nová hodnota rizika
R1	Zdržení při integraci mzdového systému	Mzdová agenda může zůstat prozatím oddělená od nového IS, přičemž tento modul se zneaktivní.	3	1	**3**
R2	Ztráta dat při transportu databází	Vícestupňové zálohování na externí cloud.	1	2	**2**
R3	Systém má po spuštění prodlevy	Složité řešení, příčin může být více. Zabránit tomu může posílení cache na straně serveru (u hostingu) popř. optimalizace některých modulů.	1	3	**3**
R4	Systém má po spuštění výpadky	Zajistit kvalitního poskytovatele hostingu s garantovanou dostupností serverů, ideálně monitorovanou externí firmou.	1	5	**5**

R5	E-shop s benefity je finančně neudržitelný	Celou koncepci distribuce benefitů je třeba koncipovat na nejhorší scénáře a tomu přizpůsobit nastavení "obchodu" tak, aby se nemusely měnit podmínky po jeho spuštění.	1	3	**3**
R6	Lidé si stěžují na gamifikační systém	Gamifikaci je vhodné nastavit zpočátku velmi nepatrně a nastavení celého systému konzultovat s odborníky.	1	2	**2**
R7	Uživatelé systém příliš nevyužívají	Chybné nastavení celého systému, procesů či gamifikačního systému. Je třeba náznaky tohoto problému odhalit ještě v rámci betatestu.	1	4	**4**
R8	Odchod IT pracovníka zodpovědného za provoz	Zajistit zastupitelnost pracovníka - tj. vyžadovat veškeré přístupy a detailní dokumentaci provedených změn (log).	2	1	**2**
R9	Zaměstnanci neví, jak se systémem pracovat	Nepodcenit úvodní zaškolení zaměstnanců a vzdělávat uživatele pravidelně - např. co se týče aktualizací. Umožnit uživatelům včasnou podporu/helpdesk.	3	1	**3**
R10	Nastane vážný bezpečnostní incident	Oblast IB zahrnuje celou škálu hrozeb, proti kterým je třeba přijmout protiopatření. Základem úspěšného řízení rizika (nejen) v IT oblasti je identifikace aktiv a hrozeb. Vypracovat DRP.	2	4	**8**

Po aplikaci návrhů opatření dojde ke snížení hodnoty rizika u všech rizik. Nejnižší hodnotu mají rizika R2 a R6 (2), nejvyšší pak R10, avšak s téměř poloviční výslednou hodnotou.



Graf č. 4: Pavučinový graf hodnot rizika
(Zdroj: autor)

Z pavučinového grafu vyplývá, že u všech rizik došlo po aplikaci opatření k poklesu jejich hodnoty. Relativně nejmenší změny přitom nastaly v případě R1 a R5, kde došlo k redukci rizika o 25 %. Největší změny se naopak týkají R9, kde došlo k redukci rizika o 75 %.

4.2.3 Ekonomické zhodnocení navrhovaných změn

Hlavním cílem finanční části projektu je finančně vyčíslit, kolik bude zavedení změny, tj. implementace vyvinuté aplikace CSRnet firmu stát. Přínosy této změny, resp. jejich značná část, je zejména nepeněžního charakteru. Vzhledem k tomu, že se jedná primárně o HRM portálový systém, přínosy projektu se projeví zejména ve zefektivnění některých procesů, jmenovitě např. v oblasti školení, dotazování a distribuce benefitů, a tedy ve výsledné úspoře času pracovníků společnosti. Část přínosů je tedy značně obtížně finančně kvantifikovatelná. Obdobné je to i s výdaji na tuto změnu. Vzhledem k tomu, že se jedná o cloudovou aplikaci, instalace byla již součástí fáze vývoje a většinu implementace hodlá společnost provést ve vlastní režii, opět je zde tedy velký

podíl nemateriální složky a oportunitních nákladů. Odhadované výdaje jsou uvedeny v tabulce níže. Pozn.: Pořizovací cena samotné aplikace zde není uvedena.

Tabulka č. 18: Jednorázově vynaložené počáteční náklady na projekt
(Zdroj: autor)

Provedená činnost	Jednorázové počáteční náklady
Doprogramování mzdového modulu ext. dodavatelem	80 000 Kč
Práce IT technika – iniciace IS	30 000 Kč
Modifikace po betatestu (značně variabilní odhad)	40 000 Kč
Úvodní zaškolení odpovědných pracovníků na práci s tímto softwarem	10 000 Kč
Zřízení dočasného helpdesku pro uživatele	30 000 Kč
SUMA	**190 000 Kč**

Tabulka č. 19: Roční (pravidelné) náklady na IS
(Zdroj: autor)

Provedená činnost	Roční náklady
Hosting aplikace	20 000 Kč
Pravidelná údržba a aktualizace	14 000 Kč
Drobné modifikace (odhad)	30 000 Kč
SUMA	**64 000 Kč**

Roční náklady se již netýkají pouze fáze implementace, ale budou se vynakládat během celé životnosti projektu, resp. fungování IS. Jedná se zejména o výdaje na hosting aplikace (připomínám, že se jedná o webovou platformu) a dále pravidelnou údržbu a aktualizace dílčích modulů nutné pro zajištění informační bezpečnosti IS.

4.2.4 Časová analýza

V časové analýze je použita metoda PERT umožňující snazší vyjádření nejistoty a nepřesnosti odhadů délky trvání. Součástí časové analýzy je i vyhotovení síťového grafu s uzlově definovanými uzly. Cílem této časové analýzy je mj. nalezení kritické cesty (metoda CPM), tedy té, kde jsou minimální, resp. nulové časové rezervy.

4.2.4.1 Časový harmonogram změny

Na počátku projektu je třeba definovat zodpovědné osoby podílející se na projektu samotném a schválit rozpočet implementace. Zásadním klíčovým milníkem je spuštění demo verze, načež bude možné začít souběžně realizovat hned několik činností. Bude nutné vyřešit nastavení gamifikačního systému, a to jak z hlediska ekonomického, tak psychologického. Je také třeba řešit dodatečný požadavek na integraci se systémem na

zpracování mezd a tvorbu benefitů, tedy těch, které jsou způsobilé pro tento způsob distribuce. Současně bude postupně nahráván obsahu e – learningu, stejně jako již hotových dotazníků. Následně započne fáze betatestování na vybraných zaměstnancích podniku – jak řadových pracovníků, tak manažerů. Aplikaci bude nutné následně upravit dle nalezených neshod a chyb. Další činností bude vyhotovení seznamu uživatelů, pro které se musí definovat jasná a zřejmá pravidla používání, stejně jako bude vhodné vytvořit uživatelskou dokumentaci pro urychlení orientace v systému. Následující činnosti zahrnují migraci mzdových dat a nastavení přístupových práv dle jednotlivých uživatelských rolí. Bude nutné zaškolit jak manažery, tak řadové zaměstnance a následně zajistit bezpečnou distribuci přihlašovacích údajů směrem k nim. Pro dosažení zdařilé implementace je také vhodné ustanovit osobu na niž se mohou v případě potíží se systémem uživatelé obracet. Jakmile jsou tyto kroky splněné, bude možné oficiálně zahájit provoz a po určité době vyhodnotit úspěšnost implementace. Bude vhodné zjišťovat spokojenost uživatelů s používáním podnikového portálu například pomocí metodiky B2EPUS s využitím dotazníkového šetření.

Tabulka č. 20: Časový harmonogram projektu
(Zdroj: autor)

Údaje o postupnosti činností projektu				Trvání [dny]				Statistické ukazatele		Termíny zahájení a ukončení činností				Rezerva
Činnost	**Popis činnosti**	**i**	**j**	**a**	**m**	**b**	**t(ij)**	**σ2**	**σ**	**ZM**	**KM**	**ZP**	**KP**	**RC**
A	Schválení rozpočtu, def. zodp. osob a vymez. kompet.	-	B	2	5	14	6,0	4,00	2,00	0,00	6,00	0,00	6,00	**0,0**
B	Konfigurace esenciálního nastavení administrátorem	A	C	3	7	14	7,5	3,36	1,83	6,00	13,50	6,00	13,50	**0,0**
C	Spuštění testovací demo verze	B	D,E,F,G	5	10	15	10,0	2,78	1,67	13,50	23,50	13,50	23,50	**0,0**
D	Tvorba nastavení gamifikačního systému	C	H,L	4	12	25	12,8	12,25	3,50	23,50	36,30	55,20	68,00	31,7
E	Integrace se systémem na zpracování mezd	C	H,L	1	8	20	8,8	10,03	3,17	36,30	45,10	59,20	68,00	22,9
F	Tvorba benefitů způsobilých pro distribuci e-shopem	C	H,L	20	30	50	31,7	25,00	5,00	36,30	68,00	36,30	68,00	**0,0**
G	Nahrání obsahu e-learningu a dotazníků	C	H,L	3	8	10	7,5	1,36	1,17	36,30	43,80	60,50	68,00	24,2
H	Příprava testovacího prostředí (na betatest)	D,E,F,G	I	1	2	5	2,3	0,44	0,67	68,00	70,30	68,00	70,30	**0,0**
I	Betatest na vybraných zaměstnancích	H	J	30	35	40	35,0	2,78	1,67	70,30	105,30	70,30	105,30	**0,0**
J	Úprava IS dle výsledků betatestu, odstranění chyb	I	K,L	1	15	60	20,2	96,69	9,83	105,30	125,50	105,30	125,50	**0,0**
K	Vyhotovení seznamu uživatelů	J	M	1	2	4	2,2	0,25	0,50	125,30	127,50	130,50	132,70	5,2
L	Definování pravidel používání IS, tvorba int. směrnic	D,J	M	3	7	12	7,2	2,25	1,50	125,50	132,70	125,50	132,70	**0,0**
M	Tvorba uživatelské dokumentace	K,L	N	8	14	25	14,8	8,03	2,83	132,70	147,50	132,70	147,50	**0,0**
N	Migrace mzdových dat do IS	M	O	1	2	4	2,2	0,25	0,50	147,50	149,70	147,50	149,70	**0,0**
O	Nastavení přístupových práv	N	P,Q,R	1	2	3	2,0	0,11	0,33	149,70	151,70	149,70	151,70	**0,0**
P	Zaškolení koncových uživatelů – manažeři	O	S	4	7	10	7,0	1,00	1,00	151,70	158,70	163,40	170,40	11,7
Q	Zaškolení koncových uživatelů – zaměstnanci	O	S	10	18	30	18,7	11,11	3,33	151,70	170,40	151,70	170,40	**0,0**
R	Příprava strategie spuštění	O	S	2	4	8	4,3	1,00	1,00	151,70	156,00	166,10	170,40	14,4
S	Aktivace uživatelských účtů	P,Q,R	T,U	1	2	4	2,2	0,25	0,50	170,40	172,60	170,40	172,60	**0,0**
T	Bezpečná distribuce přihl. údajů mezi pracovníky	S	V	1	3	5	3,0	0,44	0,67	172,60	175,60	175,60	178,60	3,0
U	Zřízení helpdesku v souvislosti se spuštěním IS	S	V	4	6	8	6,0	0,44	0,67	172,60	178,60	172,60	178,60	**0,0**
V	Oficiální spuštění IS	T,U	W	1	2	3	2,0	0,11	0,33	178,60	180,60	178,60	180,60	**0,0**
W	Vyhodnocení úspěšnosti spuštění IS	V	-	5	14	30	15,2	17,36	4,17	180,60	195,80	180,60	195,80	**0,0**

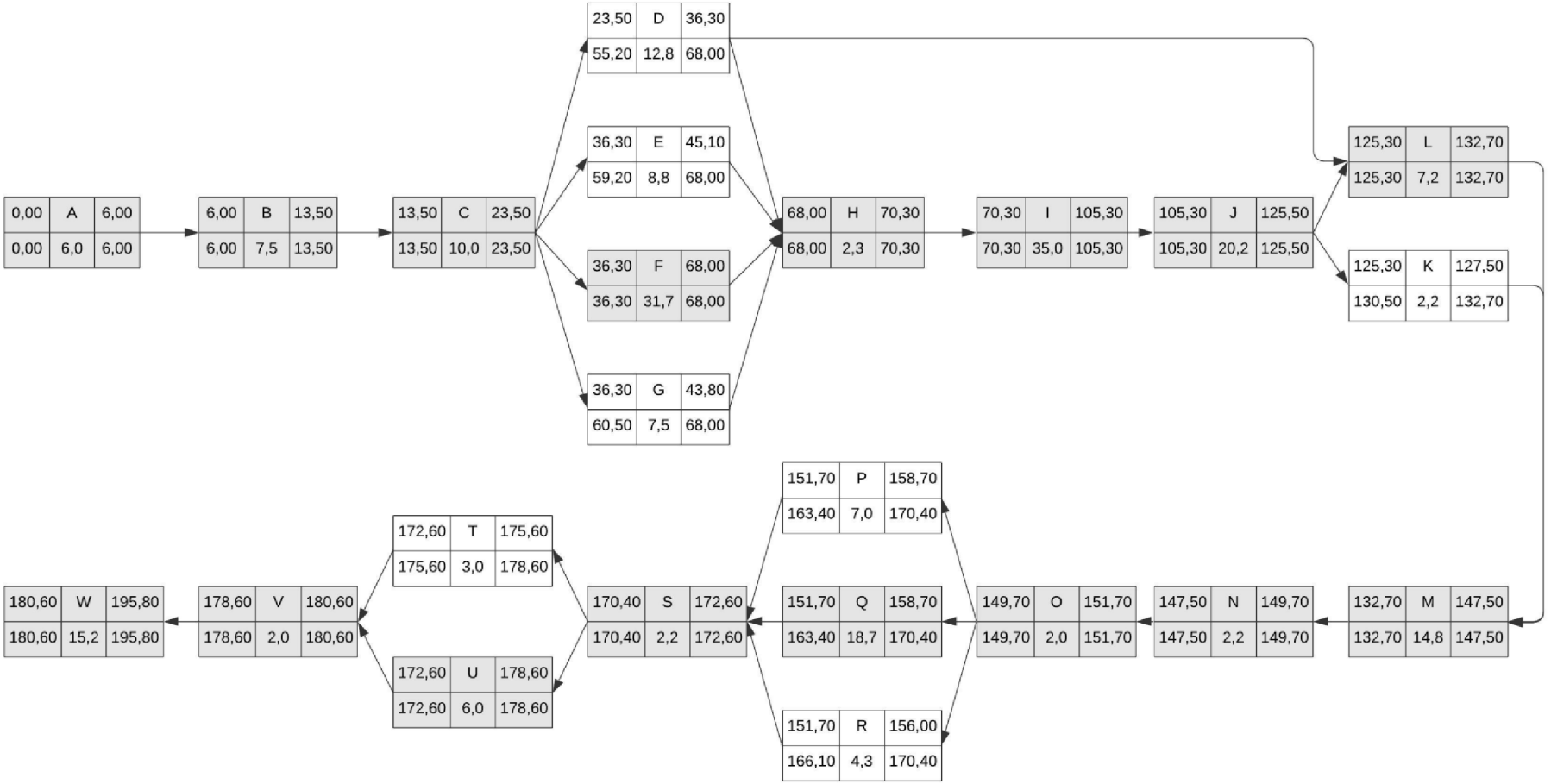
4.2.4.2 Síťový graf PERT

Na základě tabulky níže byl vyhotoven uzlově definovaný síťový graf (SG) PERT s následujícím rozložením uzlu:

Tabulka č. 21: Použité rozložení uzlu
(Zdroj: autor)

ZM	OA	KM
ZP	t_e	KP

Kde: OA – označení činnosti; t_e – střední doba trvání; ZM, KM – začátek možný, konec možný; ZP, KP – začátek přípustný, konec přípustný. Kritická cesta, tj. cesta, kde je nulová časová rezerva je označena v grafu výše. Jedná se o body (činnosti): A-B-C-F-H-I-J-K-M-N-O-Q-S-U-V-W. Kritická cesta je dlouhá 183 dní, což se může jevit jako relativně dlouhá doba potřebná k implementaci cloudové aplikace, nicméně je třeba brát v potaz předchozí zkušenosti podniku s implementací IS, resp. pokusy o implementaci.



Graf č. 5: Síťový graf PERT
(Zdroj: autor)

4.2.5 Shrnutí plánu implementace

Implementací aplikace CSRnet, by kromě zefektivnění některých procesů (distribuce výplatnic, školení zaměstnanců atp.) došlo také ke zvýšení angažovanosti pracovníků a posílení firemní kultury, což by v delším horizontu potenciálně mohlo vést i k nižší fluktuaci na některých pracovištích. Kritická cesta projektu vychází na přibližně 183 dní – časový plán projektu je třeba přizpůsobit tempu ve firmě, zvláště, když implementace probíhá ve vlastní režii. V současné době se podnik také potýká s menšími personálními nedostatky, resp. značným personální vytížením a obecně horší kvalitou řízení projektů a vznikajícími časovými průtahy. Není také moudré provádět více změn najednou, což klade jednak větší náročnost na projektové řízení, které je, jak již bylo několikrát zmíněno, v předmětném podniku slabší. Vše je navíc umocněno specifickou situací sociálního podniku, kde jsou povětšinou zaměstnanci obecně náchylnější k negativním dopadům změn (což však není vždy pravidlem). Je tedy nutné k provádění rozsáhlejších změn v podniku postupovat s ohledem na zaměstnance zvlášť obezřetně a citlivě. Pomocí analýzy rizik byla identifikována nejzávažnější rizika projektu, na která by se měla společnost obzvláště zaměřit. Největší identifikované riziko spadá do kategorie informační bezpečnosti a je jím hrozba ztráty či kompromitace citlivých dat v systému obsažených.

4.3 Návrhy změn dle aplikací

Níže jsou představeny návrhy na zlepšení na základě zjištění vyplývajících z provedených analýz a aktuálně řešených nedostatků. Tyto dílčí návrhy se týkají jednotlivých aplikací podnikového IS, jako je Synology Drive a Aplikace Třídírna.

4.3.1 Synology Drive

Data aplikace Synology Drive jsou uložena lokálně na NAS v brněnské centrále společnosti, odkud jsou v pravidelných intervalech (denně) zálohována na cloud, konkrétně na Synology C2 Storage. Ochrana lokálních dat je řešena také zrcadlením (mirroring) pevných disků (tj. RAID 1). Sdílené síťové úložiště však nemá zálohované napájení (UPS), takže **v případě výpadku či odstávky elektřiny nebude mít společnost přístup k souborům**. Výpadek dodávek elektrické energie v budově by měl

za následek také přerušení internetového připojení, jelikož společnost sdílí v pronajaté kanceláři a síťové prvky vně kanceláře, resp. celá síťová infrastruktura není zálohovaná. Tento problém s NAS lze vyřešit několika způsoby.

K NAS je možné tento záložní AP připojit skrze druhé rozhraní LAN, jelikož předmětný model NAS je vybaven dvěma porty. Záložní LTE modem by byl taktéž zálohovaný prostřednictvím UPS. Takovýto set by **poskytl ochranu jak před výpadkem internetového připojení, tak i výpadkem elektrické sítě.** V této variantě je tedy kalkulováno s pořízením 4G (LTE) modemu (pořizovací cena přibližně 2000 Kč bez DPH) a měsíčního tarifu s neomezeným FUP, který činí, na základě aktuálního podnikového ceníku od operátora přibližně 300 Kč (bez DPH). Pro zálohování elektrické energie je možné využít kompatibilní UPS od výrobců např. APC nebo EATON, kde je dle Synology zaručena kompatibilita (Synology Incorporated, c2022). Takovýto UPS vychází přibližně na 5000 Kč (bez DPH), přičemž umožňuje překlenutí provozu (při odhadovaném proudovém odběru NAS a modemu) v řádu desítek minut. Toto řešení je vhodné v případě oblastí s četnými krátkodobými výpadky vyvolanými nestabilitou sítě, což však není případ Brna. Při delším výpadku budou data na NAS po určité době nedostupná. Značně dražším řešením je použití baterie s větší kapacitou – např. **UPS schopné s těmito odběrovými parametry překlenout přibližně dvouhodinový výpadek se prodává za cca 20000 Kč** (bez DPH). V tomto kontextu je možné zanedbat náklady na spotřebu elektřiny modemu, je však stále nutné připočíst **náklady na záložní internetové připojení ve výši přibližně 3600 Kč (bez DPH) ročně**. Je zde však stále přítomné riziko, že pokud se nepodaří dodávky služeb obnovit za daný čas, podniková data nebudou dostupná.

Tabulka č. 22: Pořizovací náklady varianty modemu a UPS
(Zdroj: autor)

Položka	**Orientační náklady**
LTE modem	2 000 Kč
UPS	20 000 Kč
Doplňkový spotřební materiál	1 000 Kč
Montáž	1 000 Kč
SUMA	**25 000 Kč**

Druhou variantou je pořízení druhého NAS na pražskou nebo hradeckou pobočku a tím i snížení pravděpodobnosti, že data nebudou v požadovaný okamžik dostupná. Toto

řešení však také klade vyšší požadavky na fyzické zabezpečení zařízení umístěného v dané lokalitě. Obdobný **model NAS vybavený obdobnými disky stojí přibližně 15000 Kč** (bez DPH). V případě nedostupnosti jednoho NAS se provoz automaticky přesměruje na druhé zařízení ve fyzicky oddělené lokalitě. Tato varianta řešení vyžaduje využití služby Synology Hybrid Share (jedná se o tzv. cross-site synchronizaci), což vyžaduje přechod na Advanced plan v C2 Storage za přibližně 1700 Kč/rok (bez DPH). V ceně je zahrnut i 1 TB prostoru na cloudu navíc. (Synology C2, c2022) Změna by tedy představovala **roční navýšení o cca 1450 Kč, oproti současnému plánu Basic** za přibližně 250 Kč ročně (bez DPH). Toto řešení by také mj. přineslo zrychlení doby odezvy při přístupu přes internet, tj. z jiných lokalit než z brněnské centrály.

Obe navrhované varianty je **možné realizovat velice rychle**, maximálně během jednoho dne, tudíž **chod podniku naruší pouze minimálně**. V obou případech také pracovníci, resp. uživatelé IS nepocítí takřka žádné negativní změny. Ze srovnání variant vychází podstatně **výhodněji druhá varianta, tj. pořízení druhého zařízení NAS a jeho umístění do geograficky oddělené lokality**, čímž se mj. dosáhne i snížení doby odezvy při přístupu z ostatních poboček. Tato varianta ke svému fungování vyžaduje upgrade na Advanced plan v C2 Storage, v kontextu podniku se však nejedná o nijak významnou částku. Varianta pořízení druhého NAS má nejen nižší pořizovací náklady a také poloviční roční periodické náklady.

4.3.2 Aplikace Třídírna

Mezi nedostatky této BI aplikace patří vyjma občasného pomalejšího načítání, což je dáno zřejmě zejména možnostmi server-side processingu v rámci sdíleného hostingu, hlavně problém s vypovídající hodnotou poskytovaných dat prostřednictvím dashboardů a generovaných reportů. Možnosti operaci s daty jsou přímo v aplikaci poměrně omezené, proto se v současné době data v pravidelných intervalech stahují a importují do MS Excel k další analýze, přičemž tento proces je dělán ručně na týdenní bázi pověřeným pracovníkem.

Aplikaci je pochopitelně možné přeprogramovat či doprogramovat, resp. rozšířit o možnost generování sestav přímo z aplikace (resp. z webového prohlížeče) a přidat některé grafy na dashboardy, což je však poměrně značný zásah do její stávající

struktury s odhadovanou cenou v řádově desítkách tisíc korun. V souvislosti s tím by bylo vhodné docílit většího propojení databází napříč podnikem.

Další možnost, která se přímo nabízí a je relativně snadná a rychle proveditelná je **propojení s MS Power BI**. Aplikaci Power BI lze relativně snadno napojit přímo na databázi MySQL (storage enigine MyISAM), v níž jsou uložená data třídírny. Cena této aplikace je **okolo 200 Kč za uživatele na měsíc** (Microsoft Power BI, c2022). Power BI nabízí daleko pokročilejší výstupy oproti Excelu a umožňuje značně zefektivnit práci s daty. Tato varianta vyžaduje vytvořit v online administraci hostingu nového uživatele pro danou databázi. Power BI Desktop vyžaduje stažení komponenty MySQL Connector pro připojení k databázi MySQL. Celý proces propojení databáze je v tomto případě otázkou maximálně několik desítek minut a nevyžaduje provádění žádných změn na straně Aplikace Třídírna. Úspory tohoto řešení spočívají zejména ve značné **úspoře času pracovníka ručně stahujícího data a provádějícího analýzy v MS Excel**. Vzhledem k nutnosti zobrazování těchto reportů na minimálně týdenní bázi bude odhadovaná časová úspora přibližně 4-5 hodin měsíčně, což se nemusí jevit jako výrazná úspora, avšak hlavní přínos této změny spočívá v podrobnější analýze provozních dat a **zkvalitnění nynějších značně omezených podkladů pro rozhodování**. Zapracování tohoto návrhu přinese zkvalitnění rozhodovacích procesů, jelikož Power BI umožňuje pokročilejší práci s daty, a především bude možné zvýšit frekvenci posuzování výkonnosti zaměstnanců třídírny, což přináší i možné využití na operativní úrovni řízení.

ZÁVĚR

Cílem diplomové práce bylo posoudit informační systém sociálního podniku sales24, s.r.o. a navrhnout změny vedoucí k jeho zlepšení a eliminaci nalezených rizik. V teoretické části byla představena základní východiska pro praktickou část diplomové práce a provedena literární rešerše týkající se informačních systémů a souvisejících trendů. Následně byl představen zkoumaný podnik vč. jeho okolí i některé odlišnosti, plynoucí ze specifického postavení sociálního podniku. Z provedených analýz vzešlo zjištění, že podnikový informační systém je v nerovnováze a vykazuje výrazné nedostatky především v oblasti informační bezpečnosti, což potvrdil i realizovaný primární výzkum. Nároky na procesní řízení a informační systém společně se zvětšováním firmy rostou. Podnik má za sebou změnu podnikové strategie, resp. business modelu spojenou obdobím prudkého růstu. Nyní se nachází před další výzvou v podobě implementace nového systému CSRnet. Navrženy byly také dílčí změny v jednotlivých aplikacích a opatření technického a organizačního typu. Přínosy řešení jsou zejména kvalitativního rázu, například zefektivnění některých procesů a úspora času pracovníků. Jedná se také o doporučení v oblasti managementu IS a informační a kybernetické bezpečnosti, které by měl management podniku věnovat více pozornosti, a především přistupovat k řešení IS/IT více koncepčně. Na základě zjištěných skutečností společnost podnikla kroky vedoucí k nápravě nejzávažnějších identifikovaných rizik. Realizace opatření vede ke zlepšení stavu informační bezpečnosti podniku, potažmo i ke zvýšení efektivnosti celého IS.

Mezi hlavní limity práce patří relativně nízký počet účastníků rozhovorů, což je dáno specifickým zaměřením výzkumu a organizační strukturou podniku. Je nutné uvést, že výčet identifikovaných nedostatků není konečný, jelikož některé potenciální hrozby nemusely být účastníky rozhovorů rozpoznány. Není ani trvale platný, jelikož v dynamicky se vyvíjejícím prostředí IS/IT lze pozorovat kontinuální výskyt nových hrozeb a nových požadavků kladených na IS. Pro hlubší deskripci stavu IS lze také doporučit realizaci anonymního dotazníkového šetření mezi zaměstnanci, zaměřeného na jejich osobní informační bezpečnost na pracovišti.

SEZNAM POUŽITÝCH ZDROJŮ

AHLFELDT, Rose-Mharie, Paolo SPAGNOLETTI a Guttorm SINDRE, 2007. Improving the Information Security Model by using TFI. In: *New Approaches for Security, Privacy and Trust in Complex Environments*. s. 73-84. ISBN 9780387723662.

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

BASL, Josef, 2011. *Inovace podnikových informačních systémů: podpora konkurenceschopnosti podniků*. Praha: Professional Publishing. ISBN 978-80-7431-045-4.

BOGOST, Ian, 2011. 'Gamification Is Bullshit'. *The Atlantic* [online]. AUGUST 9 , 2011 [cit. 2022-05-08]. Dostupné z: https://www.theatlantic.com/technology/archive/2011/08/gamification-is-bullshit/243338/

C2 Storage, c2022. *Synology C2* [online]. [cit. 2022-05-08]. Dostupné z: https://c2.synology.com/en-global/storage/hybrid

Ceny Power BI: Analýzy pro libovolnou organizaci, c2022. *Microsoft Power BI: Vizualizace dat* [online]. [cit. 2022-05-08]. Dostupné z: https://powerbi.microsoft.com/cs-cz/pricing/

CLASHING: Vzdělávací herní platforma v oblasti kybernetické a informační bezpečnosti (CLSH1), c2021. *ICT Pro: ICT kurzy a školení* [online]. [cit. 2022-05-08]. Dostupné z: https://www.skoleni-ict.cz/kurz/CLASHING-vzdelavaci-herni-platforma-v-oblasti-kyberneticke-a-informacni-bezpecnosti--CLSH1.aspx

ČSN EN ISO 9000. *Systémy managementu kvality - Základní principy a slovník.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011. Třídící znak 010300.

ČSÚ, 2019. *Výběrové šetření osob se zdravotním postižením* [online]. Praha, 16. 12. 2019 [cit. 2022-05-08]. Dostupné z: https://www.czso.cz/documents/10180/90600407/26000619.pdf/b1d5a2b3-a309-4412-a962-03d847d3d1a0?version=1.5

ČSÚ, 2022a. *Zaměstnanost a nezaměstnanost podle výsledků VŠPS - 1. čtvrtletí 2022* [online]. 04.05.2022 [cit. 2022-05-08]. Dostupné z: https://www.czso.cz/csu/czso/cri/zamestnanost-a-nezamestnanost-podle-vysledku-vsps-1-ctvrtleti-2022

ČSÚ, 2022b. *Inflace, spotřebitelské ceny* [online]. 11.04.2022 [cit. 2022-05-08]. Dostupné z: https://www.czso.cz/csu/czso/inflace_spotrebitelske_ceny

DOLEŽAL, Jan, Pavel MÁCHAL a Branislav LACKO, 2012. *Projektový management podle IPMA*. 2., aktualiz. a dopl. vyd. Praha: Grada. Expert (Grada). ISBN 978-80-247-4275-5.

FOTR, Jiří a Ivan SOUČEK, 2011. *Investiční rozhodování a řízení projektů: jak připravovat, financovat a hodnotit projekty, řídit jejich riziko a vytvářet portfolio projektů*. Praha: Grada. Expert (Grada). ISBN 978-80-247-3293-0.

GÁLA, Libor, Jan POUR a Zuzana ŠEDIVÁ, 2009. *Podniková informatika*. 2., přeprac. a aktualiz. vyd. Praha: Grada. Expert (Grada). ISBN 978-80-247-2615-1.

GÁLA, Libor, Jan POUR a Zuzana ŠEDIVÁ, 2015. *Podniková informatika: počítačové aplikace v podnikové a mezipodnikové praxi*. 3., aktualizované vydání. Praha: Grada Publishing. Management v informační společnosti. ISBN 978-80-247-5457-4.

GIRARD, John, 2013. Top Seven Failures in Mobile Device Security. *Gartner* [online]. 14 February 2013 [cit. 2022-05-08]. Dostupné z: https://www.gartner.com/en/documents/2337716

GIRITON: Online Docházka [online], c2021. [cit. 2022-05-08]. Dostupné z: https://giriton.com/cs

HAMARI, Juho, 2019. Gamification. *The Blackwell Encyclopedia of Sociology* [online]. G. Ritzer (Ed.) [cit. 2022-05-08]. Dostupné z: doi:10.1002/9781405165518.wbeos1321

HANÁČEK, Petr a Jan STAUDEK, 2000. *Bezpečnost informačních systémů: metodická příručka zabezpečování produktů a systémů budovaných na bázi informačních technologií*. Praha: Úřad pro státní informační systém. ISBN 80-238-5400-3.

HENNYEYOVÁ, Klára, 2017. ŠILEROVÁ, Edita a Klára HENNYEYOVÁ. *Informační systémy v podnikové praxi*. Druhé vydání. Praha: Powerprint, s. 121-143. ISBN 978-807-5680-655.

HINDLS, Richard, Stanislava HRONOVÁ a Robert HOLMAN, 2003. *Ekonomický slovník*. Praha: C.H. Beck. Beckovy odborné slovníky. ISBN 80-717-9819-3.

HUOTARI, Kai a Juho HAMARI, 2011. *"Gamification" from the perspective of service marketing* [online]. CHI'2011 (Gamification workshop) [cit. 2022-05-08]. Dostupné z: https://www.researchgate.net/publication/267942356_Gamification_from_the_perspective_of_service_marketing

CHVÁTALOVÁ, Zuzana a Miloš KOCH, 2015. Optimizing of Information Systems in Companies: Support of Sustainable Performance. *Procedia - Social and Behavioral Sciences* [online]. 213, 842-847 [cit. 2022-05-08]. ISSN 18770428. Dostupné z: doi:10.1016/j.sbspro.2015.11.488

Interaktivní online kurzy INSTRUCTOR, c2022. *INSTRUCTOR: Česká jednička nejen pro online školení BOZP a PO* [online]. [cit. 2022-05-08]. Dostupné z: https://www.instructor.cz/online-kurzy

ISACA, 2010. *The Business Model for Information Security* [online]. [cit. 2022-05-08]. Dostupné z: https://store.isaca.org/s /store#/store/browse/detail/a2S4w000004Ko8cEAC

JIROUŠ, Filip, 2019. *Čínský systém sociálního kreditu jede. "Hříšníci" hůře hledají partnera i práci* [online]. [cit. 2021-11-02]. Dostupné z: https://sinopsis.cz/cinsky-system-socialniho-kreditu-jede-hrisnici-hure-hledaji-partnera-i-praci/

JOHNSON, Dave, 2021. What is software? A guide to all of the different types of programs and applications that tell computers what to do. *Insider* [online]. Mar 26, 2021 [cit. 2022-05-07]. Dostupné z: https://www.businessinsider.com/what-is-software

KEMP, Chris, 2014. *Will BYOD Become 'Bring Your Own Cloud?'* [online]. April 01, 2014 [cit. 2022-05-08]. Dostupné z: http://www.informationweek.com/cloud/infrastructure-as-a-service/will-byod-become-bring-your-own-cloud/d /d-id/1141602

KLAPZTEIN, Sol a Carla CIPOLLA, 2016. *From Game Design to Service Design* [online]. 47(5), 566-598 [cit. 2022-05-08]. ISSN 1046-8781. Dostupné z: doi:10.1177/1046878116641860

KOĎOUSKOVÁ, Barbora, 2022. *UX a UI design: Jak na uživatelské rozhraní webů a aplikací?* [online]. 08.02.2022 [cit. 2022-05-08]. Dostupné z: https://www.rascasone.com/cs/blog/ux-design-ui-design

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

Kolibřík CSRteam: řešení HR kapacit a snížení mzdových nákladů [online], c2022. [cit. 2022-05-08]. Dostupné z: https://kolibrikcsr.cz/

KOSOUR, Zdeněk, obchodní ředitel [ústní sdělení]. Brno, 16.12.2021.

KUMAR, Janaki Mythily, Mario HERGER a Rikke FRIIS DAM, 2020. *Bartle's Player Types for Gamification* [online]. [cit. 2022-05-08]. Dostupné z: https://www.interaction-design.org/literature/article/bartle-s-player-types-for-gamification

KUNSTOVÁ, Renata, 2009. *Efektivní správa dokumentů: co nabízí Enterprise Content Management*. Praha: Grada. Management v informační společnosti. ISBN 978-802-4732-572.

LAKSHMI, Sree, 2017. DMS Vs ECM - The Similarities and Differences. *Medium* [online]. Oct 17, 2017 [cit. 2022-05-07]. Dostupné z:

https://medium.com/@srilxmi.k /dms-vs-ecm-the-similarities-and-differences-e0e3a2c2840

LAUDON, Kenneth C. a Jane P. LAUDON, 2005. *Management Information Systems: Managing The Digital Firm*. 9th Edition. Prentice Hall. ISBN 9780131538412.

LIEBEROTH, Andreas, 2015. Shallow Gamification: Testing Psychological Effects of Framing an Activity as a Game. *Games and Culture* [online]. 10(3), 229-248 [cit. 2021-11-02]. ISSN 1555-4120. Dostupné z: doi:10.1177/1555412014559978

MELL, Peter a Timothy GRANCE, 2011. *The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology* [online]. Gaithersburg: National Institute of Standards and Technology [cit. 2022-05-08]. Dostupné z: doi:10.6028/NIST.SP.800-145

MOLNÁR, Zdeněk, 2001. *Efektivnost informačních systémů*. 2. rozš. vyd. Praha: Grada. Management v informační společnosti. ISBN 80-247-0087-5.

MOORE, G. A. Dealing with Darwin: How great companies innovate at every phase of their evolution. New York: Penguin Group, 2008. 281 s. ISBN: 978-1-59184-214-9.

NOVOTNÝ, Štěpán. 2022. Analýza a zhodnocení stavu informační bezpečnosti ve společnosti sales24, s.r.o. *Podnikání a management v kontextu 21. století: Vybrané research papers studentů magisterského studijního programu Strategický rozvoj podniku*. (IN PRESS).

Oslo Manual 2018. 2018-10-22. Dostupné z: doi:10.1787/9789264304604-en

Programové prohlášení vlády [online]. Praha, 7. 1. 2022 [cit. 2022-05-08]. Dostupné z: https://www.vlada.cz/cz/programove-prohlaseni-vlady-193547/

REDMAN, Thomas C., 2008. *Data Driven: Profiting from Your Most Important Business Asset* [online]. Harvard Business School Publishing [cit. 2022-05-07]. ISBN 9781422119129.

REŽŇÁKOVÁ, Mária, 2012. *Efektivní financování rozvoje podnikání*. Praha: Grada. Finance (Grada). ISBN 978-80-247-1835-4.

ROSICKÝ, Antonín. 2010. Člověk: informace a znalost. Informační management. Praha: Professional Publishing, s. 53-80. ISBN 978-80-7431-010-2.

ROWLEY, J. E. a Richard HARTLEY, c2008. *Organizing knowledge: an introduction to managing access to information*. 4th ed. Burlington: Ashgate. ISBN 978-0-7546-4431-6.

ROWLEY, Jennifer, 2007. The wisdom hierarchy: representations of the DIKW hierarchy. *Journal of Information Science* [online]. 33(2), 163-180 [cit. 2022-05-07]. ISSN 0165-5515. Dostupné z: doi:10.1177/0165551506070706

Seznam kompatibilních produktů Synology, c2022. *Synology Incorporated* [online]. [cit. 2022-05-08]. Dostupné z: https://www.synology.com/cs-cz/compatibility?search_by=category&category=upses&p =1 &change_log_p =1

SCHWALBE, Kathy, 2007. *Řízení projektů v IT*. Brno: Computer Press. Kompletní průvodce (Computer Press). ISBN 978-80-251-1526-8.

SCHWALBE, Kathy, 2011. *Řízení projektů v IT: kompletní průvodce*. Brno: Computer Press. ISBN 978-80-251-2882-4.

SMEJKAL, Vladimír a Karel RAIS, 2013. *Řízení rizik ve firmách a jiných organizacích*. 3., rozš. a aktualiz. vyd. Praha: Grada. Expert (Grada). ISBN 978-802-4730-516.

SODOMKA, Petr a Hana KLČOVÁ, 2010. *Informační systémy v podnikové praxi*. 2., aktualiz. a rozš. vyd. Brno: Computer Press. ISBN 978-802-5128-787.

SVOZILOVÁ, Alena, 2011. *Zlepšování podnikových procesů*. Praha: Grada. Expert (Grada). ISBN 978-80-247-3938-0.

SYNEK, Miloslav, 2001. *Manažerská ekonomika*. 2. přeprac. a rozš. vyd. Praha: Grada. Expert (Grada). ISBN 80-247-9069-6.

ŠILEROVÁ, Edita, 2017. ŠILEROVÁ, Edita a Klára HENNYEYOVÁ. *Informační systémy v podnikové praxi*. Druhé vydání. Praha: Powerprint, s. 13-120. ISBN 978-807-5680-655.

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

VÁCHAL, Jan a Marek VOCHOZKA, 2013. *Podnikové řízení*. Praha: Grada. Finanční řízení. ISBN 978-80-247-4642-5.

VEBER, Jaromír a Jitka SRPOVÁ, 2012. *Podnikání malé a střední firmy*. 3., aktualiz. a dopl. vyd. Praha: Grada. Expert (Grada). ISBN 978-80-247-4520-6.

Většina českých zaměstnanců je poctivá. Online docházku proto obvykle vítají, říká Střeš z Giritonu, 2017. *Zprávy z VUT* [online]. 4. září 2017 [cit. 2022-05-08]. Dostupné z: https://www.zvut.cz/napady-objevy/napady-a-objevy-f38103/vetsina-ceskych-zamestnancu-je-poctiva-online-dochazku-proto-obvykle-vitaji-rika-gres-z-giritonu-d149847

WALZ, Steffen P. a Seabastian DETERDING, 2015. *The Gameful World: Approaches, Issues, Applications*. Cambridge: MIT Press. ISBN 9780262028004.

YOUNG, Carl S., 2016. *Information Security Science* [online]. 2016 [cit. 2022-04-26]. Dostupné z: doi:10.1016/C2015-0-05918-4

Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, 2004. In: *Sbírka zákonů*. částka 173.

ZEFIS - audit informačních systémů [online]. [cit. 2021-12-15]. Dostupné z: https://zefis.cz/

SEZNAM POUŽITÝCH OBRÁZKŮ

SEZNAM POUŽITÝCH TABULEK

SEZNAM POUŽITÝCH GRAFŮ