



**VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ**

BRNO UNIVERSITY OF TECHNOLOGY

**FAKULTA PODNIKATELSKÁ**

FACULTY OF BUSINESS AND MANAGEMENT

**ÚSTAV INFORMATIKY**

INSTITUTE OF INFORMATICS

## **POSOUZENÍ INFORMAČNÍHO SYSTÉMU FIRMY A NÁVRH ZMĚN**

INFORMATION SYSTEM ASSESSMENT AND PROPOSAL OF ICT MODIFICATION

**DIPLOMOVÁ PRÁCE**

MASTER'S THESIS

**AUTOR PRÁCE**

AUTHOR

**Bc. MAREK LINNER**

**VEDOUCÍ PRÁCE**

SUPERVISOR

**doc. Ing. MILOŠ KOCH, CSc.**

**BRNO 2024**

# Zadání diplomové práce

Ústav: Ústav informatiky  
Student: **Bc. Marek Linner**  
Vedoucí práce: **doc. Ing. Miloš Koch, CSc.**  
Akademický rok: 2023/24  
Studijní program: Informační management

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 2023/24

V Brně dne 4.2.2024

L. S.

---

doc. Ing. Miloš Koch, CSc.  
garant

---

doc. Ing. Vojtěch Bartoš, Ph.D.  
děkan

## Abstrakt

Diplomová práce se zaměřuje na posouzení informačního systému vybrané společnosti a návrhy, jak zlepšit jeho vlastnosti. Úvodní teoretická část práce představuje problematiku informačních systémů, uživatelského rozhraní a informační bezpečnosti. V následující kapitole jsou rozvinuty analýzy současného stavu informačního systému. Třetí kapitola identifikuje nalezené nedostatky, pro které navrhuje i řešení. Poslední čtvrtá kapitola vyhodnocuje návrhy z ekonomického pohledu.

## Abstract

The thesis focuses on assessing the information system of a selected company and proposes ways to improve its capabilities. The introductory theoretical part of the thesis presents issues related to information systems, user interfaces, and information security. In the following chapter, analyses of the current state of the information system are elaborated. The third chapter identifies issues and suggests solutions. The final chapter evaluates the proposals from an economic perspective.

## Klíčová slova

Porterův model, PEST, informační systém, ZEFIS, informační bezpečnost, ERP

## Keywords

Porter's Five Forces, PEST, information system, ZEFIS, information security, ERP

## Citace

LINNER, Marek. *Posouzení informačního systému firmy a návrh změn*. Brno, 2024. Dostupné také z <https://www.vutbr.cz/studenti/zav-prace/detail/158626>. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce doc. Ing. Miloš Koch, CSc.

# Posouzení informačního systému firmy a návrh změn

## 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).

.....

Marek Linner

26. května 2024

## Poděkování

Obrovské poděkování patří především mému vedoucímu doc. Ing. Miloši Kochovi, CSc., za jím strávený čas, zpětnou vazbu a nesmírně cenné rady. Dále chci poděkovat zaměstnancům společnosti ABC za poskytnuté podklady pro analýzy a možnost s nimi spolupracovat.

Další poděkování míří k mým nejbližším. Mé rodině za podporu a poskytovanou stabilitu při studiu a mé přítelkyni za psychickou podporu a trpělivost v náročných chvílích.

Poslední poděkování ponechávám sám sobě – za čas strávený studiem, za snahu vynaloženou při zpracování projektů a za odhodlání studium úspěšně dokončit.

# Obsah

|          |                                                                        |           |
|----------|------------------------------------------------------------------------|-----------|
| <b>1</b> | <b>Úvod</b>                                                            | <b>6</b>  |
| <b>2</b> | <b>Cíle práce</b>                                                      | <b>7</b>  |
| <b>3</b> | <b>Teoretická východiska práce</b>                                     | <b>8</b>  |
| 3.1      | Data . . . . .                                                         | 8         |
| 3.2      | Informace . . . . .                                                    | 9         |
| 3.3      | Znalost . . . . .                                                      | 10        |
| 3.4      | Informační systém . . . . .                                            | 10        |
| 3.4.1    | Struktura informačního systému . . . . .                               | 10        |
| 3.4.2    | Informační systémy a jejich klasifikace . . . . .                      | 11        |
| 3.4.3    | Životní cyklus informačních systémů . . . . .                          | 12        |
| 3.4.4    | Podnikové informační systémy . . . . .                                 | 14        |
| 3.5      | Informační bezpečnost . . . . .                                        | 15        |
| 3.6      | Analýza PEST . . . . .                                                 | 16        |
| 3.7      | Porterova analýza pěti sil . . . . .                                   | 18        |
| 3.8      | Analýza pomocí portálu ZEFIS . . . . .                                 | 20        |
| 3.9      | User experience . . . . .                                              | 22        |
| 3.10     | User interface . . . . .                                               | 22        |
| 3.11     | Zálohování . . . . .                                                   | 24        |
| <b>4</b> | <b>Analýza současného stavu</b>                                        | <b>28</b> |
| 4.1      | Popis analyzované společnosti . . . . .                                | 28        |
| 4.2      | Popis zkoumaného informačního systému Infosys . . . . .                | 28        |
| 4.2.1    | Moduly Infosysu a jejich uživatelské rozhraní . . . . .                | 29        |
| 4.2.2    | Technické specifikace Infosysu . . . . .                               | 40        |
| 4.3      | Porterova analýza pěti sil . . . . .                                   | 44        |
| 4.4      | PEST analýza . . . . .                                                 | 47        |
| 4.5      | Analýza metodou ZEFIS . . . . .                                        | 51        |
| <b>5</b> | <b>Identifikace nedostatků a návrhy vylepšení informačního systému</b> | <b>59</b> |
| 5.1      | Identifikace a rozbor nalezených nedostatků . . . . .                  | 59        |
| 5.1.1    | Zaměstnancům je umožněno manipulovat s cizími soubory . . . . .        | 59        |
| 5.1.2    | Rizika spojená s ochranou osobních údajů zaměstnanců . . . . .         | 59        |
| 5.1.3    | Chybí šifrování úložiště . . . . .                                     | 60        |
| 5.1.4    | Ruční nastavování jednotlivých práv každému uživateli . . . . .        | 60        |
| 5.1.5    | Nedostatečně časté zálohování dat z MS Access souborů . . . . .        | 61        |
| 5.1.6    | Nezastupitelnost externího tvůrce systému . . . . .                    | 61        |

|          |                                                                |           |
|----------|----------------------------------------------------------------|-----------|
| 5.1.7    | Překlepy a chyby v textu uživatelského rozhraní . . . . .      | 61        |
| 5.2      | Návrhy na zlepšení současného stavu . . . . .                  | 62        |
| 5.2.1    | Úprava firemních procesů v souladu s GDPR . . . . .            | 62        |
| 5.2.2    | Zavedení uživatelských skupin . . . . .                        | 63        |
| 5.2.3    | Zavedení šifrování dat na disku . . . . .                      | 65        |
| 5.2.4    | Vylepšení uživatelského rozhraní . . . . .                     | 66        |
| 5.2.5    | Zvýšení frekvence zálohování textových dat MS Access . . . . . | 67        |
| 5.2.6    | Odvrácení dopadů neoprávněných zásahů do souborů . . . . .     | 67        |
| <b>6</b> | <b>Ekonomické vyhodnocení navržených řešení</b>                | <b>68</b> |
| 6.1      | Vyhodnocení očekávaných přínosů . . . . .                      | 68        |
| 6.1.1    | Vyhodnocení finančních přínosů . . . . .                       | 68        |
| 6.1.2    | Vyhodnocení nefinančních přínosů . . . . .                     | 69        |
| 6.2      | Vyhodnocení očekávaných nákladů . . . . .                      | 69        |
| <b>7</b> | <b>Závěr</b>                                                   | <b>72</b> |
|          | <b>Literatura</b>                                              | <b>73</b> |

# Seznam obrázků

|      |                                                                                                                                                                                                                                                                                                                                                                                                                                           |    |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| 3.1  | Proces transformace dat na informaci. Zdroj: vlastní zpracování podle [29]. . . . .                                                                                                                                                                                                                                                                                                                                                       | 9  |
| 3.2  | Pyramida znázorňující úrovně informačního systému. Zdroj: [30]. . . . .                                                                                                                                                                                                                                                                                                                                                                   | 11 |
| 3.3  | Životní cyklus informačního systému. Zdroj: vlastní zpracování. . . . .                                                                                                                                                                                                                                                                                                                                                                   | 12 |
| 3.4  | Dělení informačních systémů. Zdroj: [17]. . . . .                                                                                                                                                                                                                                                                                                                                                                                         | 14 |
| 3.5  | Důvěrnost, dostupnost a integrita v rámci informační bezpečnosti. Zdroj: [13].                                                                                                                                                                                                                                                                                                                                                            | 15 |
| 3.6  | Základní přehled vlivů makrookolí působící na firmy rozdělený do čtyř oblastí tak, jak s nimi nakládá analýza PEST. Zdroj: [28]. . . . .                                                                                                                                                                                                                                                                                                  | 18 |
| 3.7  | Porterův model pěti sil. Zdroj: vlastní zpracování podle [15]. . . . .                                                                                                                                                                                                                                                                                                                                                                    | 19 |
| 3.8  | Příklad výstupu analýzy portálem ZEFIS. Zdroj: [40]. . . . .                                                                                                                                                                                                                                                                                                                                                                              | 21 |
| 3.9  | Základní rozdíly mezi user experience a user interface. Zdroj: [32]. . . . .                                                                                                                                                                                                                                                                                                                                                              | 23 |
| 3.10 | Diagram zobrazující různé strategie při procesu zálohování dat. Zdroj: vlastní zpracování podle [39]. . . . .                                                                                                                                                                                                                                                                                                                             | 24 |
| 4.1  | Rozcestníkový banner, který se otevře jako první okno po spuštění Infosysu. Obsahuje tlačítka v horní liště pro nastavení samotného systému a 7 dalších tlačítek pro spuštění jednotlivých modulů. Žlutě zabarvená místa zobrazují jméno přihlášeného uživatele a jméno tvůrce systému. Zdroj: vlastní zpracování.                                                                                                                        | 29 |
| 4.2  | Okno modulu Docházka Infosysu. V levé části pracovníci zadávají datum, čas příchodu do práce a čas odchodu. V pravé části zaměstnanci zaznamenávají informace o tom, jakým činností se věnovali, po jakou dobu a na které zakázce pracovali. Žlutě zabarvená místa zakrývají název zakázky, jméno přihlášeného uživatele a jméno tvůrce systému. Zdroj: vlastní zpracování. . .                                                           | 30 |
| 4.3  | Okno modulu Firmy. V horní liště mohou zaměstnanci přidávat, mazat, řadit, vyhledávat a kategorizovat záznamy do oddělených seznamů. Ve spodní části obrazovky mohou pracovníci upravovat již existující zvolený záznam a na spodním kraji mohou přepínat mezi podsekcemi modulu. Žlutě zabarvená místa zakrývají přehled informací o kontaktech, jméno přihlášeného uživatele a jméno tvůrce systému. Zdroj: vlastní zpracování. . . . . | 31 |

- 4.4 Ukázka okna modulu Zakázky. V horní liště mohou zaměstnanci mimo jiné vyhledávat, procházet, tisknout nebo ukládat provedené změny. V levé polovině obrazovky se nachází textová pole, pomocí kterých může uživatel zobrazit nebo upravit detailní informace o zvolené zakázce, jejím objednateli, odpovědné osobě, časovém plánu, finanční rekapitulaci nebo může procházet spárovanou výkresovou dokumentaci. V pravé části je vyobrazen seznam všech zakázek s několika málo základními informacemi o nich, přičemž detaily může uživatel vidět a upravovat v levé části po rozkliknutí požadovaného záznamu zakázky. Vlevo dole se pak nachází tlačítka sloužící k přepínání mezi podmoduly a vpravo dole seznam všech vytvořených dokumentů, které jsou spojeny s danou zakázkou. Žlutě zabarvená místa zakrývají názvy a další informace z přehledu zakázek vpravo, detailní záznamy o zvolené zakázce v levé části, jméno přihlášeného uživatele a jméno tvůrce systému. Zdroj: vlastní zpracování. . . . . 33
- 4.5 Ukázka obrazovky modulu Výkresy. V horní liště může oprávněný uživatel procházet, přidávat, mazat či hledat požadovaný výkres. V levé části obrazovky se nachází detailní informace o konkrétním výkresu, jakými jsou například název, autor, typ, popis a další. V pravé části okna modulu se pak zobrazuje kompletní list všech existujících výkresů s několika málo nejdůležitějšími informacemi o něm – pro zobrazení či úpravu všech detailních informací stačí výkres v pravém okně označit a informace vlevo podle vůle upravit a uložit. Žlutě zabarvená místa zakrývají názvy a další informace z přehledu výkresů vpravo, detaily zvoleného výkresu v levé části, jméno přihlášeného uživatele a jméno tvůrce systému. Zdroj: vlastní zpracování. . . . . 34
- 4.6 První okno podmodulu Výrobních zakázek. V levé horní části jsou po zadání požadovaného kódu dílu zobrazeny základní informace o něm a v levé dolní části se nachází výpis lidí kteří se na něm podíleli, jakou činností a jak dlouho. Žlutá místa zakrývají skutečný název firmy ABC a jméno přihlášeného uživatele. Zdroj: vlastní zpracování. . . . . 36
- 4.7 Druhé okno podmodulu Výrobní objednávky a výroba dílů. V horní části obrazovky se nachází funkcionality spojená s prvním podmodulem výrobních objednávek, spodní část obrazovky je pak využívána k obsluze podmodulu Výroba dílů. Žlutě zabarvená místa zakrývají citlivé informace o lidech, zakázkách a klientech. Zdroj: vlastní zpracování. . . . . 37
- 4.8 Třetí okno podmodulu Řízení výrobních čísel. V levé části může uživatel pomocí textboxů upravovat informace o stávajícím záznamu, přičemž v pravé části obrazovky mu podmodul umožňuje záznamy o výrobních číslech procházet, filtrovat nebo řadit. Žlutá místa zakrývají citlivé informace o lidech, zákaznících a přesnějším popisu určení vytvořených dílů. Zdroj: vlastní zpracování. . . . . 38

|      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |    |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| 4.9  | Okno modulu Dokumenty se skládá ze tří částí – vrchní části, kde uživatel může nastavovat způsob zobrazení a filtrování již existujících dokumentů například podle názvu, typu nebo autora. Prostřední část obrazovky zabírá prostor pro samotné zobrazení požadovaných informací, tedy listu vytvořených dokumentů a jejich attributech. Zobrazují se informace jako datum vzniku, číslo dokumentu, jméno autora, číslo zakázky nebo adresovaná firma. Ve spodní části obrazovky je uživatel schopen vytvořit dokument nový – vybere pomocí záložek lišty požadovaný typ dokumentu, vyplní náležité informace, zvolí jazyk dokumentu a po stisknutí tlačítka VYTVOŘENÍ Infosys vygeneruje úplně nový dokument s unikátním číslem. Žlutě zabarvená místa zakrývají přehled dokumentů, jméno přihlášeného uživatele a jméno tvůrce systému. Zdroj: vlastní zpracování. . . . . | 41 |
| 4.10 | Ukázka okna modulu Persons. V horní liště mohou vedoucí zaměstnanci přidávat a mazat jednotlivé záznamy, v pravé části obrazovky se nachází sekce umožňující úpravy existujících záznamů. Prostřední část pak zobrazuje samotná data o všech současných i bývalých zaměstnancích. Žlutě zabarvená místa zakrývají přehled osobních informací, jméno přihlášeného uživatele a jméno tvůrce systému. Zdroj: vlastní zpracování. . . . .                                                                                                                                                                                                                                                                                                                                                                                                                                         | 42 |
| 4.11 | Vývoj inflace v České republice podle údajů Českého statistického úřadu. Zdroj: [7]. . . . .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 48 |
| 4.12 | Vývoj cen pohonných hmot v České republice podle údajů Českého statistického úřadu. Zdroj: [8]. . . . .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 49 |
| 4.13 | Vývoj ceny energií v Evropské unii podle údajů Evropské rady. Na svislé ose je srovnání hodnoty s cenou v roce 2015, tzn. pokud graf zobrazuje hodnotu 200, je cena energie na 200 % oproti ceně v roce 2015. Zdroj: [4]. . . . .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 50 |
| 4.14 | Výstup systému ZEFIS obsahující analýzu nedostatků. Červeně označeny jsou závažné chyby, žlutě označeny jsou chyby se středním dopadem a zeleně vyznačené jsou méně důležité nedostatky. Zdroj: [16]. . . . .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 51 |
| 4.15 | Výsledek efektivnosti informačního systému. Hodnoty na osách jsou udávány v procentech, fialová čára značí efektivitu v jednotlivých oblastech a modře vyplněná oblast značí celkovou úroveň efektivitu informačního systému. Zdroj: [16]. . . . .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 56 |
| 4.16 | Detailní výsledky efektivnosti metody ZEFIS. Zdroj: [16]. . . . .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 57 |
| 4.17 | Výsledek bezpečnosti informačního systému. Hodnoty na osách jsou udávány v procentech, světle červená čára značí bezpečnost v jednotlivých oblastech a tmavě červeně vyplněná oblast značí celkovou úroveň bezpečnosti informačního systému. Zdroj: [16]. . . . .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 58 |
| 4.18 | Tabulka s detailními výsledky bezpečnosti metody ZEFIS. Zdroj: [16]. . . . .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 58 |
| 6.1  | Přehled finančních benefitů, které jednotlivé vylepšení přinášejí. Zdroj: vlastní zpracování. . . . .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 69 |
| 6.2  | Přehled nefinančních benefitů, které jednotlivé vylepšení přinášejí. Zdroj: vlastní zpracování. . . . .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 70 |
| 6.3  | Přehled očekávaných nákladů. Sloupec s částkou zahrnuje jak náklady na mzdy, tak fixní náklady. Zdroj: vlastní zpracování. . . . .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 71 |

# Kapitola 1

## Úvod

V posledních letech se stále častěji stává, že interagujeme s informačními systémy natolik frekventovaně, že si to často ani neuvědomujeme. Spolu se stálým rozvojem a pokrokem v oblasti informačních technologií je vhodné informačním systémům věnovat stejnou pozornost. Kvalitně implementovaný a pečlivě udržovaný informační systém je totiž skvělým způsobem, jak zvýšit efektivitu a usnadnit práci zaměstnancům, kteří jej využívají. Bohužel v praxi se nezdá stávat, že je situace opačná. Dobře fungující informační systém společnosti je schopen v konkurenčním prostředí poskytnout výhody a posílit postavení firmy ve svém odvětví.

Současně je podceňována bezpečnost informačních systémů, protože nepřináší prakticky žádnou přidanou hodnotu a implementace bezpečnostních opatření často vyžaduje změny v zaběhnutých procesech. Problematika informační bezpečnosti je několikrát zmiňovaným tématem této diplomové práce kladoucí si za cíl posoudit informační systém společnosti a navrhnout změny.

V první teoretické kapitole práce jsou definovány a rozvinuty základní pojmy, jakými jsou například data nebo informace. Podrobněji se věnují informačním systémům jako takovým a jejich uživatelským rozhraním. Představuje i analýzy, jejichž zpracování obsahuje následující kapitola.

Druhá kapitola analyzuje současnou situaci, v jaké se nachází společnost ABC. Rozebírá detailně její informační systém Infosys i pomocí portálu ZEFIS a popisuje její makrookolí pomocí Porterova modelu pěti sil a analýzy PEST.

Následující kapitola identifikuje analýzami odhalené nedostatky, popisuje hrozby které představují a představuje možné kroky, které může ABC podniknout pro jejich mitigaci.

Poslední kapitola se věnuje návrhům a rozvádí potřebné náklady spolu s přínosy, které jejich implementace přinese.

## Kapitola 2

### Cíle práce

Cílem diplomové práce je nejprve představit společná teoretická východiska a poté na nich postavit analýzu současného stavu interního informačního systému jménem Infosys vybrané společnosti vystupující pod pseudonymem ABC. Na základě provedených analýz jsou pak zpracovány návrhy možných způsobů, jak nalezené nedostatky odstranit. V poslední kapitole práce se nachází ekonomické zhodnocení vytvořených návrhů z pohledu nákladů a získané přidané hodnoty pro firmu ABC.

## Kapitola 3

# Teoretická východiska práce

První kapitola diplomové práce se věnuje teorii a definicím dále užívaných pojmů. Tento jejich popis tvoří společný základ, na kterém staví další kapitoly práce. Obsahuje nejen vysvětlení pojmů jako jsou data, informace, znalosti, nýbrž obsahuje i popis nástrojů využitých k analýze jako je portál ZEFIS, analýza PEST nebo Porterův model pěti sil. V neposlední řadě se věnuje i popisu informačních systémů jako takových, jejich klasifikaci, struktuře, uživatelskému rozhraní a životnímu cyklu.

### 3.1 Data

Data (z latinského *datum*, něco daného) v rámci informatiky znamenají zaznamenanou hodnotu takovým způsobem, aby bylo možné je dále zpracovat počítačem. Data slouží například pro zaznamenání událostí, metrik a skutečností, avšak samy o sobě nemají žádnou vypovídající hodnotu. Data "7.3.2024, Praha, 14, JZ" nic neřeknou, dokud k nim není přiřazen kontext, jenž zmíněné hodnoty dá do souvislosti. V tomto případě, jsou-li data zasazena do kontextu měření rychlosti a síly větru, vzniknou nová, interpretovaná data – informace. Pro náš příklad získáme z dat informaci, jenž tvrdí *7. března 2024 v Praze foukal jihovýchodní vítr o síle 14 km/h*.

Data lze dále dělit do dvou kategorií podle toho, v jakém formátu jsou uchovávány[29]:

- **Strukturovaná data**

U takových dat lze jednoduše rozlišit jaký atribut, fakt nebo objekt datová hodnota popisuje. Pro člověka jsou čitelné, je pro něj mnohem snazší se v nich zorientovat a pokud zná kontext v jakém se data sbírají, je schopen z nich získávat informace. Příkladem strukturovaných dat jsou záznamy v databázových systémech, CSV (comma separated values) soubory nebo Excelovské tabulky. Pomocí počítače je pak velmi snadné nad nimi provádět agregace, zkoumání jejich vlastností nebo pokročilá statistická analýza.

- **Nestrukturovaná data**

Nestrukturovaná data se od těch strukturovaných liší tím, že se často jedná spíše o tok bytů nebo textové dokumenty, které nemají předepsanou formu a bez specializovaného softwaru je práce s nimi náročná nebo až nemožná. Jako tok bitů informací jsou reprezentovány videa, zvukové stopy nebo obrázky, mezi nestrukturované textové dokumenty můžeme řadit například životopisy nebo texty příspěvků na sociálních sítích.

Oba formáty dat mají své výhody a nevýhody a pro oba existuje řada nástrojů, které práci s nimi usnadňují[29].

Další způsob dělení dat je na interní a externí:

- **Interní data**

Interní data jsou zaznamenávány organizací, která je dále využívá pro své vlastní potřeby. Často se na ně vztahují bezpečnostní předpisy, jenž mají zabránit jejich volnému šíření. Jedná se například o osobní údaje zaměstnanců, data o prodejkách nebo záznamy o zákaznících[17].

- **Externí data**

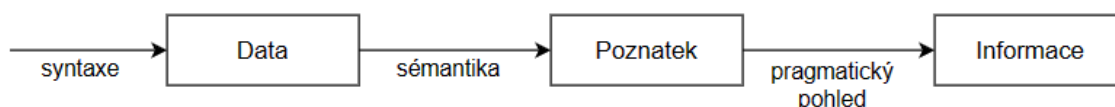
Externí data, na rozdíl od dat interních, vznikají mimo organizaci a slouží jako vstup. Lze mezi ně řadit široké spektrum hodnot, od úrovně vody v přehradě, přes statistiky počtu obyvatel až po zveřejňované finanční výkazy konkurence[17].

Data v informatice tvoří pevný konkrétní základ, na kterém dále budujeme informace a znalosti. V praxi se jim věnují pracovníci zaměření na jejich sběr, analýzu nebo datové architekti zabývající se technickou stránkou jejich uchovávání.

## 3.2 Informace

Pojem informace (z latinského *informatio*, dodávat tvar, zobrazovat) je využíván a definován v mnoha oborech lidské činnosti, například v programování, managementu nebo elektroinženýrství. V kontextu této diplomové práce využijme definici pojmu podle Rainera Kuhlena: „*Informace je podmnožina poznatků, která je někým použita v konkrétní situaci pro řešení problémů*“[19].“

Nahlédneme-li na informace z hlediska jejich vyhledávání, je možné získat již o něco konkrétnější představu. Uvedme situaci, kdy existuje databázový systém obsahující pouze hodnoty bez dalšího kontextu (sémantiky) – data. Po připojení potřebné sémantiky dat, lze z dat nově získat konkrétní *poznatky* jenž zapadají do databázového modelu. Teprve z poznatků lze na pragmatické úrovni tvořit informace[29]. Jinými slovy, vztah mezi poznatkem a informací lze formulovat tím, že informace jsou poznatky v akci. Celý tento řetězec postupné transformace dat až na informace znázorňuje obrázek 3.1.



Obrázek 3.1: Proces transformace dat na informaci. Zdroj: vlastní zpracování podle [29].

Použijeme-li příklad s měřením rychlosti větru v sekci 3.1, můžeme strukturovat data do sloupečků *datum*, *místo*, *rychlost* a *směr*. Pokud ale člověk nahlízející do tabulky neumí česky, bez *znalosti* češtiny jsou to pro něj jen data. I Čech si ale může mylně domnívat, že datum měření je udáváno v jiném formátu, místo 7. března si tedy může myslet že měření proběhlo 3. července. Vidíme zde, že při získávání informací z dat velmi důležitou roli hrají znalosti, zkušenosti a důvtip (síla větru 14 pravděpodobně neznamena ani cm/h, ani tisíce km/h)[29].

### 3.3 Znalost

Pojem znalost se dá vysvětlit jako další forma abstrakce, vzájemně související struktury poznatků. Zajímavou definici poskytli Checkland a Scholes v knize *Soft Systems Methodology in Action*:

„Technologie pracují s daty, lidé je interpretují jako informace nesoucí význam, které se stávají podnětem pro další jednání. Proces interpretace je kognitivní záležitost, ve kterém stěžejní roli hrají znalosti[5].“

Znalost tedy znamená schopnost něco reprezentovat ve svém vlastním vědomém kognitivním modelu světa a schopnost nad takovými reprezentacemi provádět další myšlenkové operace. Na jejich základě je pak nositel znalosti schopen predikovat další vývoj reálného světa[29].

Znalosti jsou základem pro vytváření nových řešení a inovací, čímž se stávají velmi lukrativní ve společnosti a na trhu práce. Disponuje-li pracovník lety zkušeností a širokou škálou znalostí, pak je schopen odvádět mnohonásobně efektivnější práci s nižší chybivostí, než člověk jenž se v daném oboru teprve vzdělává a znalosti nejsou v jeho kognitivním modelu ještě pevně ukotveny. Tomuto pohledu využití znalostí v praxi, jejich předávání, zaznamenávání a využívání se blíže věnuje *znalostí management*.

### 3.4 Informační systém

Termín systém označuje uspořádanou skupinu prvků, které mají specifické vlastnosti a vzájemné vztahy. Tyto prvky dohromady vykazují určité charakteristiky nebo chování. Informační systém pak představuje komplexní soubor lidí, technických nástrojů a metod (včetně programů), které slouží k sběru, přenosu, zpracování a uchování dat. Jeho hlavním účelem je prezentovat informace pro uživatele, kteří pracují v rámci řídicích systémů[22]. V této kapitole je představena řada aspektů informačních systémů, jako je jejich struktura, typy, životní cyklus nebo klasifikace.

#### 3.4.1 Struktura informačního systému

Informační systémy se obecně skládají z řady spolu interagujících prvků, které M. Tvrđíková rozlišuje na následujících pět kategorií:

- **Hardware**

Pojednává o fyzických přístrojích a hmotných technických prostředcích, které tvoří nosiče informačního systému jako takového. Při pořizování hardwarových prostředků je důležité dbát na to, jaké vlastnosti očekáváme – například rozhodnutí mezi koupí drahých SSD disků pro rychlé čtení dat, nebo naopak levných HDD disků s několikanásobně větším úložištěm[31].

- **Software**

Jedná se o programové vybavení, prvky systému jenž tvoří jeho nehmotnou část a které definují jeho konkrétní chování a schopnosti. Software pro daný informační systém se dá pořídit buď krabicový (již vytvořená licencovaná programová sada), lze jej vyvinout uvnitř společnosti, nebo zaplatit externí firmě za jeho tvorbu na míru[31].

- **Dataware**

Do této kategorie spadají data, informace a znalosti, jenž informační systém obsahuje. Jsou uloženy na hardwarových prvcích a s jejich zpracováním pomáhají prvky softwarové[31].

- **Peopleware**

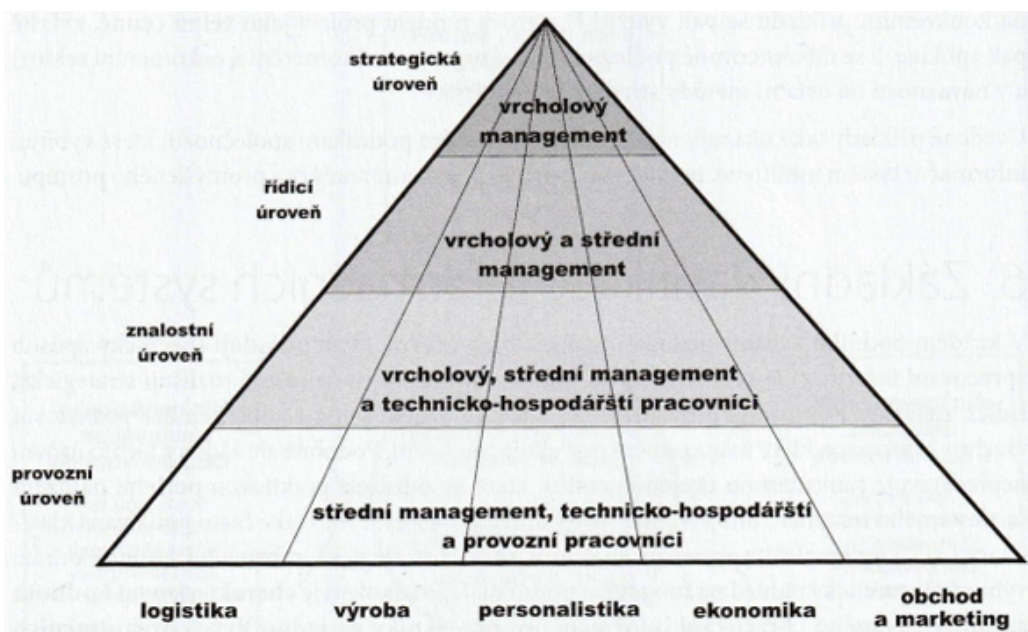
Mezi peopleware informačního systému se řadí lidé, kteří s ním nakládají – jeho uživatelé, správci, manažeři nebo vývojáři. Všichni členové peopleware by měli být proškoleni tak, aby byli schopni s IS efektivně pracovat a mohli jeho schopnosti co nejlépe využívat[31].

- **Orgware**

Poslední součástí klasifikace struktury informačního systému jsou prvky spadající pod orgware. Jedná se o sadu dokumentů popisující pravidla, pravomoci, povinnosti a postupy při práci s ním, dále obsahuje také programovou dokumentaci a bezpečnostní doporučení[31].

### 3.4.2 Informační systémy a jejich klasifikace

Jednotlivé organizační jednotky ve společnosti vyžadují pro svoji práci svůj specifický postup zpracování informací z informačního systému. Tyto pohledy lze obecně rozdělit na čtyři na sebe navazující úrovně[30], jak popisuje obrázek 3.2.



Obrázek 3.2: Pyramida znázorňující úrovně informačního systému. Zdroj: [30].

#### 1. Provozní či transakční úroveň

Na provozní úrovni systému se nejčastěji pohybují zaměstnanci na nižších pozicích obstarávající rutinní záležitosti podniku (transakce), jakými jsou například obsluha strojů nebo zaznamenávání nových informací. Klíčovými požadavky na provozní úrovni jsou přesnost, aktuálnost a dostupnost[30].

## 2. Znalostní úroveň

Sem spadají aplikace, jenž umožňují organizaci sdílet znalosti a zjednodušují jejich předávání pomocí dokumentů. Patří sem například hojně využívané aplikace sady Microsoft Office a další softwarové nástroje pro spolupráci[30].

## 3. Řídící úroveň

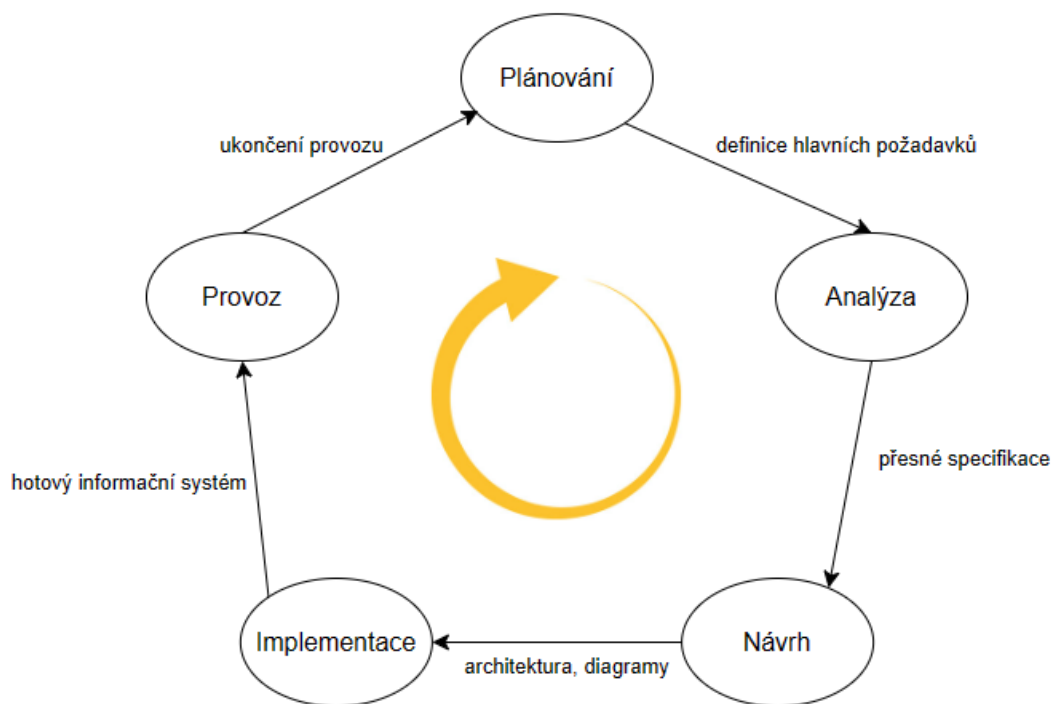
Řídící úroveň je primárně využívána k monitorování chodu společnosti pomocí výpisů a agregovaných dat a pomáhá plnit práci administrativním pracovníkům. Tato úroveň je také schopna reagovat na otázky vyššího managementu, například „kolik vadných kusů denně vyhazujeme“, „o kolik bychom museli navýšit objem výrobních surovin při koupi nového obráběcího stroje“[30].

## 4. Strategická úroveň

Nejvyšší strategická úroveň slouží exkluzivně vrcholovému managementu, protože obsahuje ty nejcitlivější informace o společnosti. Pomáhá manažerům v rozhodování a snaží se upozornit na nové trendy na trhu a jak na změny reagovat[30].

### 3.4.3 Životní cyklus informačních systémů

Podobně jako organismy nebo produkty, i informační systémy mají svůj životní cyklus. V této sekci se nachází popis cyklus jednotlivých etap existence informačního systému, od úplného začátku až po jeho vyřazení z provozu – i informační systémy stárnou a s postupem času již nedokáží splňovat neustále se měnící požadavky jeho uživatelů[18] (viz obrázek 3.3).



Obrázek 3.3: Životní cyklus informačního systému. Zdroj: vlastní zpracování.

## 1. Plánování

Plánování často bývá nejdůležitější fáze života informačního systému. Během této části probíhá primárně komunikace s koncovým zákazníkem, zjišťování relevantních informací o něm a identifikace jeho potřeb. Pokud se plánování nevěnuje dostatek času a pozornosti, může nastat situace, kdy dojde k nepochopení mezi uživateli a vývojáři, kteří poté navrhnu a implementují produkt, který nesplňuje požadavky zákazníků a neobsahuje všechnu potřebnou funkcionalitu, což výrazně snižuje kvalitu provedení, spokojenost zákazníka a zvyšuje náklady. Výstupem fáze plánování jsou dokumenty definující hlavní potřeby a problémy spolu s možnostmi jejich řešení[18].

## 2. Analýza požadavků uživatelů

V této fázi se tvůrci věnují hlavně upřesňování a detailní analýze potřeb zákazníka. Jsou s ním konzultovány první náčrty systému, zpracovávání zpětné vazby a identifikace možných úskalí v dalších fázích životního cyklu. Výsledkem fáze je tentokrát již co nejpřesnější sada dokumentace požadavků[18].

## 3. Návrh

Zde již hlavní roli sehrávají tvůrci informačního systému. Jejich úkolem je vybrat vhodné softwarové nástroje pro jeho tvorbu, vhodné hardwarové nosiče, návrh architektury zdrojových kódů a návrh finální podoby již implementovaného systému. Výstupem návrhu je řada softwarových a hardwarových specifikací, diagramy popisující architekturu budoucí implementace a popisy toho, jak bude reálný informační systém fungovat[18].

## 4. Implementace systému

Proces implementace, tedy realizace vytvořených plánů, v sobě nese řadu úkolů a kroků. Je třeba implementovat navržený kód, dokoupit chybějící hardware, připravit hotový softwarový produkt na servery zprostředkující jeho služby, nainstalovat klienty na koncové stanice a to vše důkladně otestovat – ideálně na úrovni softwaru, hardwaru a integračních testů mezi jednotlivými komponenty. Součástí této životní fáze je také tvorba podrobné softwarové dokumentace systému, seznamování uživatelů s ní a jejich školení. Na konci fáze implementace by měl systém být otestován, zdokumentován, nainstalován a zaměstnanci připraveni na práci s ním[18].

## 5. Provoz

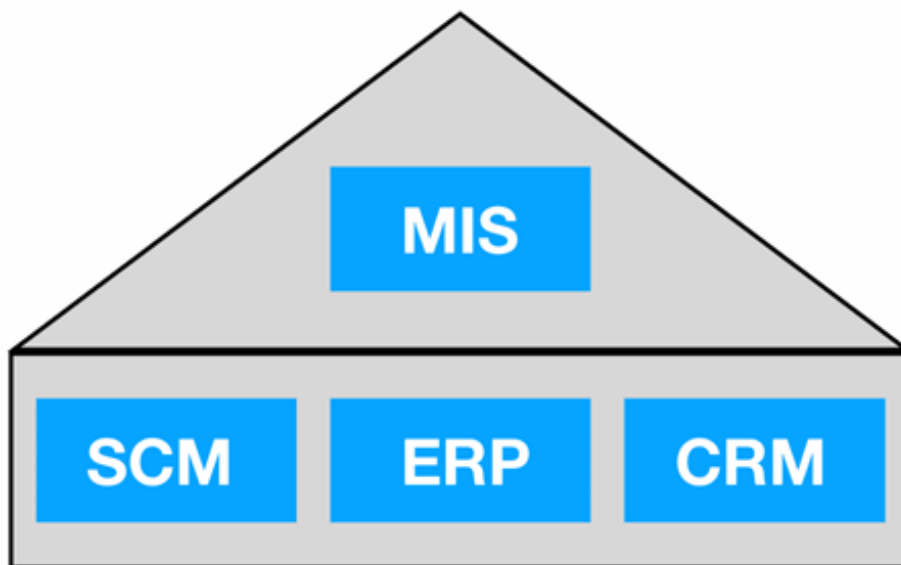
Nasazení do provozu často začíná bok po boku již stávajícího řešení, kdy správci systému pozorně kontrolují jeho správnou funkcionalitu a výstupy. Je sbírána zpětná vazba od uživatelů a základě jejich interních nebo externích vlivů (například nová legislativa) tvůrci chystají a nasazují aktualizace. Fáze provozu by měla zabrat ideálně co největší porci času životního cyklu informačního systému[18].

Z popisu životního cyklu lze poznat, že pro zákazníka je jeho pořízení a zavedení časově i finančně velmi náročné, avšak není dobrou praxí po letech jeho provozu stále trvat na jeho údržbě. Namísto toho by měla společnost kriticky na systém pohlížet a usuzovat, zda nastal čas pro jeho ukončení a nahrazení systémem novým.

### 3.4.4 Podnikové informační systémy

„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[30].“

Informační lze dále dělit podle jejich účelu na systémy *Enterprise Resource Plannig (ERP)*, *Supply Chain Management (SCM)*, *Customer Relationship Management (CRM)* a *Management Information System (MIS)*. Všechny tyto typy systémů rozvádí a popisuje následující výčet a obrázek, viz 3.4:



Obrázek 3.4: Dělení informačních systémů. Zdroj: [17].

- **ERP – Enterprise Resource Planning**

Jedná se o sofistikovaný informační systém, který se specializuje na správu interních datových toků v rámci firmy, jehož hlavním cílem je propojení a koordinace procesů probíhajících uvnitř organizace. ERP sbírá a zpracovává data tak, aby byla okamžitě dostupná uživatelům systému[30].

- **SCM – Supply Chain Management**

Supply Chain Management systémy se zabývají koordinovanou spoluprací mezi kontaktními subjekty, které společně tvoří dodavatelský řetězec. SCM se zabývá všemi procesy v tomto řetězci, od logistických a dopravních problémů až po tok informací a řízení finančních a materiálních zdrojů. Integrace SCM do informačních systémů umožňuje efektivní zrychlení celého dodavatelského procesu[26].

- **CRM – Customer Relationship Management**

Customer Relationship Management systémy vznikají díky skutečnosti, že udržet si stávající zákazníky je finančně výrazně méně náročné, nežli získat nové zákazníky. Proto řada firem zavádí CRM – soubor strategií a postupů, které společnost aplikuje při jednání a řízení vztahů se svou klientelou[2].

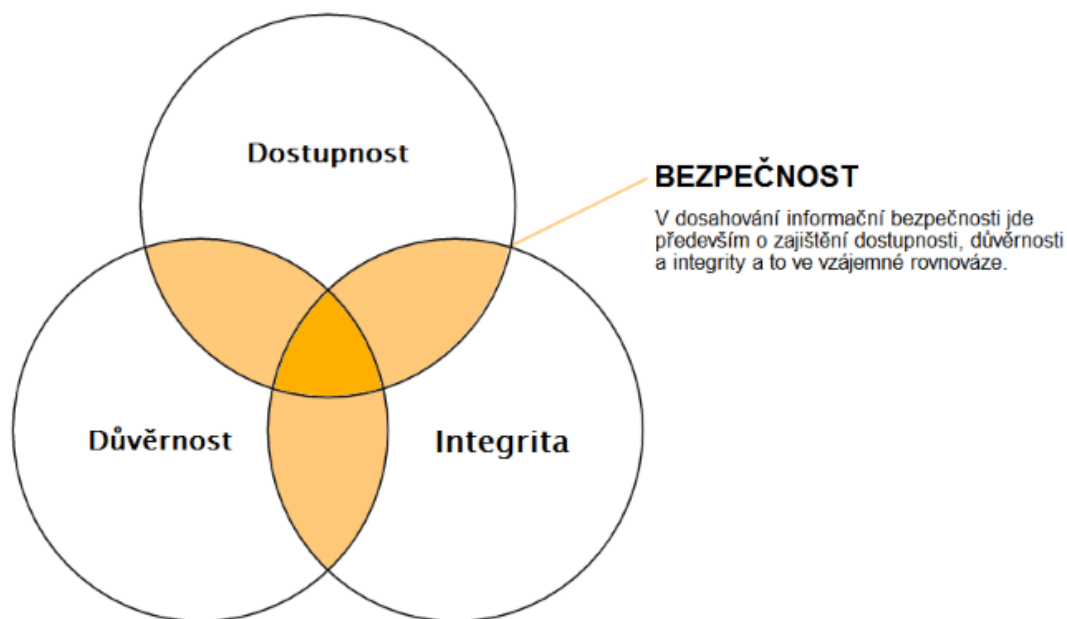
CRM systémy lze dále dělit na tři typy: *analytický*, jenž na základě extraktů dat pomáhá tvořit analýzy pro podporu rozhodování vyššího managementu, *operativní*, který se věnuje běžným procesům orientovaným k zákazníkům (prodeje, zákaznická podpora apod.) a *kooperační* CRM systémy – ty zajišťují ve velkých firmách sdílení informací a dat o zákaznících, čímž zabráňují duplikaci informací a zlepšují stav báze dat.

- **MIS – Management Information System**

Management Information System slouží vyššímu managementu. Jeho úkolem je sbírat data z celé společnosti, agregovat je a pomocí metod business intelligence tvořit výpisy sloužící k podpoře informovaného rozhodování[17].

### 3.5 Informační bezpečnost

Pod pojmem informační bezpečnosti je obecně chápán soubor technik a postupů, jejichž cílem je systém a informace v něm chránit před externími vlivy a zamezit tak případnému poškození či ztátě, zajistit chod systému a chránit data před hrozbami[24]. Bezpečnost systému a informací zaštiťují tři klíčové vlastnosti, které jsou rozvedeny v následujících podsekcích – jsou jimi důvěrnost, dostupnost a integrita[10], viz obrázek 3.5.



Obrázek 3.5: Důvěrnost, dostupnost a integrita v rámci informační bezpečnosti. Zdroj: [13].

- **Důvěrnost**

Aspekt důvěrnosti se věnuje přístupu k datům obsaženým v informačním systému. Pro data by měl být stanoven stupeň citlivosti, na jehož základě pak systém může rozhodovat, zda data uživateli poskytne či nikoliv, například pomocí uživatelských skupin a jejich oprávnění. Za důvěrný můžeme označit takový informační systém, který poskytuje data pouze osobám s přístupovými právy[24].

- **Dostupnost**

Dostupný informační systém je takový systém, jenž je schopen svým uživatelům poskytnout data v přiměřeném čase. Cílem designéra a majitele informačního systému je pak zajištění co největší dostupnosti a vyhýbání se jejího narušení vlivem softwarových a hardwarových chyb nebo útoků z vnějšího prostředí společnosti[24].

- **Integrita**

Pojem integrity v kontextu informační bezpečnosti se váže k samotnému obsahu dat. Systém by totiž měl zajišťovat a vynucovat mechaniky, kterými udrží svoji bázi dat ve správném stavu a chránit je před zanesení chyb, ať už úmyslně či neúmyslně[24]. Tomu lze pomoci například správným nastavením omezení databázových tabulek, pravidelnými kontrolami správnosti dat (*data quality inspection*) a správným využíváním vlastností jednotlivých typů transakcí, které dnešní systémy správy dat nabízejí.

Je důležité mít na paměti, že i když systém splňuje normy nebo doporučení (IEEE[11], PKCS[25], RFC[12] nebo americké FIPS[9] a ANSI[1]), je potřeba držet tempo s vývojem nových, zvláště těch softwarových, hrozeb. Je tedy dobrou praxí jednou za čas stav bezpečnosti systému zrevidovat a zajistit, že je připraven odolat i nejnovějším útokům.

### 3.6 Analýza PEST

Analýza označovaná PEST se zabývá vnějším makrookolím společnosti z pohledu čtyř faktorů – politického a legislativního, ekonomického, sociálního a technologického. Každá ze skupin v sobě obsahuje řadu faktorů, které různou měrou ovlivňují zkoumanou společnost a jejichž důležitost se mění dle toho, v jakém odvětví společnost pracuje a jaká je současná situace – odborná literatura tento přístup často označuje jako strategický audit vlivů makrookolí[14].

Následující čtyři sekce blíže popisují každou ze skupin faktorů, kterými se analýza PEST zabývá[28].

- **Politické a legislativní faktory**

Politické a legislativní faktory makrookolí představují pro společnost jak velké příležitosti, tak vážné hrozby. Dotýkají se všech podniků vlivy jakou jsou daně, cla, cenová politika, regulační politika importu a exportu zboží, antimonopolní legislativa nebo v poslední době čím dál častěji zmiňované regulační zákony pro ochranu životního prostředí a zákony týkající se sdílení a uchovávání dat (například GDPR[41]) a to nejen na úrovni České republiky, ale také na úrovni Evropské unie a jiných mezinárodních spolků. Legislativa tvoří rámec, ve kterém každý podnik musí fungovat a ač podnik může využívat možností jemu nabízených, je také nucen se řídit zákony stanovenými pravidly[28].

- **Ekonomické faktory**

Každá společnost je při svém rozhodování výrazně ovlivněna stavem ekonomiky a makroekonomickými trendy. Mezi jejich základní indikátory, které by měl podnik sledovat, patří například míra ekonomického růstu, centrální bankou stanovená úroková míra, vývoj inflace, daňová legislativa a směnné kurzy k cizím měnám, zejména euru a dolaru. Konkrétně míra ekonomického růstu ovlivňuje podnik tím, že

vyvolává rozsah a obsah příležitostí, avšak zároveň tvoří i hrozby.

Právě ekonomický růst totiž zvyšuje spotřebu a příležitosti na trhu. Podobně i úroková míra výrazně ovlivňuje výnosnost podnikání tím, že stanovuje cenu kapitálu a zhodnocení investic, naopak nízká úroková míra napomáhá podniku realizovat jeho plány. Vysoká inflace negativně působí na investiční činnosti a limituje ekonomický rozvoj a devizové kurzy významně ovlivňují konkurenceschopnost společností v zahraničí.

Všechny zmíněné indikátory jsou spolu úzce provázány a nelze je hodnotit samostatně, proto je potřeba finanční analýzy a studie provádět v jejich širším kontextu, na kterých poté podnik může stavět svoji strategii. Je vhodné také brát v úvahu stát, který lze vnímat jakožto neporazitelného a neohroženého konkurenta, jehož činnost na trhu tvoří další příležitosti a hrozby. Schopnost predikovat jeho strategii a plány mohou podniku pomoci vyhnout se střetu s ním a naopak využít prostor, který svými kroky tvoří[28].

- **Sociální a demografické faktory**

Do faktorů sociálních a demografických se projevují zejména vlivy spojené s lidmi – jejich návyky, názory, způsob života a priority a stejně jako lidská společnost se stále vyvíjí pod tlakem kultury, ekonomiky, demografických změn, náboženských postojů, vzdělání a etiky. Poznání sociálních trendů plynoucích ze snahy jednotlivců zajistit pro sebe lepší život může získat velké výhody v konkurenčním boji o zákazníky. Příkladem je využití demografického trendu stárnutí populace k rozšíření nabídky kosmetiky zaměřené pro seniory, zájem zejména mladých lidí mít více osobního času přiměl zaměstnavatele nabízet více dnů dovolené a sezónní změny v módě z podstatné části udávají, co textilní společnosti vyrábí. Schopnost takové trendy predikovat, analyzovat a jejich využití nabízí obrovské příležitosti pro prakticky každou firmu[28].

- **Technologické faktory**

V zájmu každé firmy by měla být snaha nezaostávat oproti konkurenci na technologické rovině. Je klíčové být informován o všech změnách a postupu technologie a být schopen predikovat, jaký vliv budou mít na společnost. K tomu výrazně pomohou studie zabírající se tím, jaké vlivy mají jednotlivé technologické inovace na stav vnějšího okolí, na konkurenční podniky a jaké příležitosti či hrozby přináší zkoumané firmě[28].

Výsledky analýzy PEST by měly podnítit společnost k pokládání následujících a jim podobných otázek a hledání odpovědí na ně:

1. Jak se budou vyvíjet trendy významných faktorů v budoucnosti?
2. Jaké faktory tvoří impulzy změny? Budou v budoucnu silnější nebo slabší?
3. Jaký bude dopad na podnik? Jaký budou vlivy mít dopad na konkurenci?
4. Jaký budou mít očekávané změny dopad na strategii podniku? Jak by měly být zahrnuty při její formulaci?

Odpovědi na položené otázky spolu s výsledky analýzy PEST pak zkoumané společnosti umožní mít informovanější vhled do svého vnějšího makrookolí a změn v něm působícím[28].

| <b>Politicko-legislativní faktory</b>                    | <b>Ekonomické faktory</b>       |
|----------------------------------------------------------|---------------------------------|
| Antimonopolní zákony                                     | Hospodářské cykly               |
| Ochrana životního prostředí                              | Trendy HDP                      |
| Ochrana spotřebitele                                     | Devizové trhy                   |
| Daňová politika                                          | Kupní síla                      |
| Regulace v oblasti zahraničního obchodu, protekcionismus | Úrokové míry                    |
| Pracovní právo                                           | Inflace                         |
| Politická stabilita                                      | Nezaměstnanost                  |
|                                                          | Průměrná mzda                   |
|                                                          | Vývoj cen energií               |
| <b>Sociokulturní faktory</b>                             | <b>Technologické faktory</b>    |
| Demografický vývoj populace                              | Vládní podpora výzkumu a vývoje |
| Změny životního stylu                                    | Celkový stav technologie        |
| Mobilita                                                 | Nové objevy                     |
| Úroveň vzdělání                                          | Změny technologie               |
| Přístup k práci a volnému času                           | Rychlost zastarávání            |

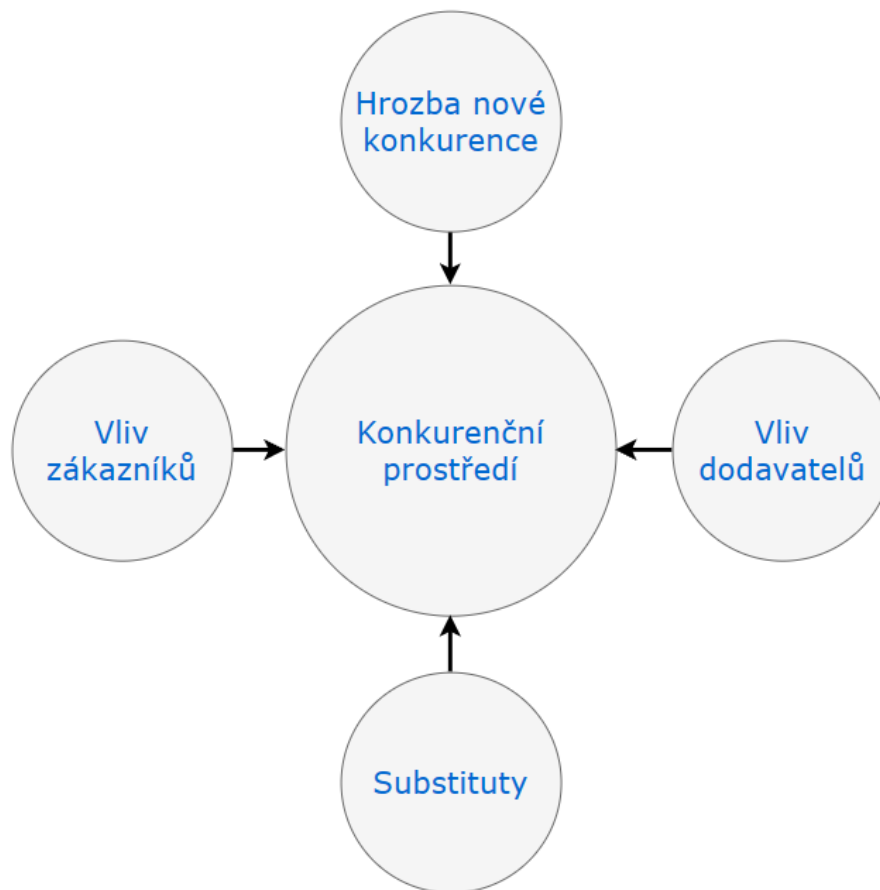
Obrázek 3.6: Základní přehled vlivů makrookolí působící na firmy rozdělený do čtyř oblastí tak, jak s nimi nakládá analýza PEST. Zdroj: [28].

### 3.7 Porterova analýza pěti sil

Jedná se o postup využívaný pro tvorbu rozboru vnějšího konkurenčního prostředí firmy, jehož výstupem je pak ucelený přehled informací o externích vlivech působící na společnost. Věnuje se zejména problematice z pohledu vyjednávací síly mezi zákazníky a dodavateli, z pohledu hrozby již existující konkurence, vzniku konkurence nové nebo hrozby substitučních produktů přítomných na trhu. Výstupem je pak identifikace nejen hrozeb, ale i příležitostí, které by analyzované firmě mohly přinést výhodu na trhu[15]. Model zjednodušeně popisuje obrázek 3.7.

#### Vyjednávací síla zákazníků

V oblasti vyjednávací síly vzhledem k zákazníkovi se Porterův model zaměřuje především na faktory jako jsou velikost poptávky po firemním produktu, zda má zákazník jednoduchou cestu jak přejít ke konkurenci, zda má snadný přístup k tržním informacím a má přehled o trhu v daném odvětví, zda je citlivý na cenu nebo zda si zákazník může vytvořit výrobek sám. Platí, že čím nižší sílu má zákazník vůči výrobcu, tím lépe pro společnost a dostává se jí více manévrovacího prostoru například v cenové politice nebo úrovni poskytnutých služeb[15].



Obrázek 3.7: Porterův model pěti sil. Zdroj: vlastní zpracování podle [15].

### Vyjednávací síla dodavatelů

Analýza z pohledu vyjednávací síly dodavatele směrem k výrobcí se věnuje převážně aspektům jako množství alternativních poskytovatelů firmou poptávaných služeb, dostupnosti tržních informací, míře specifičnosti poptávaných produktů či možnosti využití substitutů. Čím větší je vyjednávací síla dodavatele, například v případě kdy jeden dodavatel vlastní většinu trhu, tím je situace horší pro společnost. V pozici odběratele si nemůže příliš vybírat mezi produkty a pokud sama není pro poskytovatele velkým a důležitým klientem, není schopna si vyjednat lepší cenové podmínky a nezbyvá jí mnoho možností[15].

### Hrozba existující konkurence

Na prakticky každém trhu libovolného odvětví se vyskytuje vzájemná konkurence. Každý účastník daného trhu v daném odvětví se snaží získat co největší tržní podíl, ať už úrovní nabízených služeb, cenami nebo marketingem. Čím vyšší je počet rivalů, tím obtížnější bývá získat konkurenční výhodu, společnosti vynakládají více zdrojů ve vzájemném soupeření a častěji se vedou cenové války, což nahrává spíše zákazníkovi nežli poskytovatelům statků či služeb. Čím početnější a tvrdší soupeření na trhu je, tím menší sílu je schopna si vybraná společnost vydobýt[15].

## Hrozba vstupu nové konkurence do odvětví

Vstup nového rivala na trh znamená hrozbu pro každého již existujícího účastníka. Obzvlášť velká šance vzniku nové konkurence je na takových trzích, do kterých jsou malé bariéry vstupu nebo slibují lukrativní zisky. Účinným nástrojem řízení takového rizika je úmyslné držení nízkých marží prodeje, aplikace velkých úspor z rozsahu nebo zvýšení nároků, jaké musí rival překonat aby měl vůbec naději se na novém trhu udržet[15].

## Hrozba substitutů

Substitutem se rozumí takové produkty a služby, které mohou svým užitek nahradit produkty dané společnosti. Typickým příkladem jsou substituty rohlíku – v případě, kdy cena rohlíku stoupne, spotřebitelé se uchýlí k substitutům jakými jsou chléb nebo housky. Čím více substitutů pro produkt společnosti existuje, tím větší riziko pro ni představují a musí brát v potaz nejen svůj vlastní trh, ale i trh substitučních výrobků. Pokud se firma chce riziku bránit, musí učinit své produkty opravdu jedinečnými a nenahraditelnými, což ale na řadě trhů není vůbec jednoduché[15].

Stojí však za zmínku existence další třídy produktů, které se nazývají komplementy – zboží, které se kupuje společně s dalším zbožím (např. herní konzole a hry prodávané na její platformě). I komplementy mohou značně ovlivňovat trh a jejich význam by také neměl být podceňován[15].

## 3.8 Analýza pomocí portálu ZEFIS

Portál ZEFIS je elektronický konzultant, který pomáhá najít nedostatky v oblasti informačních systémů a jejich bezpečnosti. Dává uživatelům nejenom doporučení, jaké věci by bylo vhodné zlepšit, ale také ukazuje, zda a v jaké míře trpí těmito nedostatky ostatní podobné firmy[40] (viz příklad výstupu: 3.8).

Systém ZEFIS nejprve pomocí uživateli vyplněných dotazníků analyzuje společnost, její informační systémy a procesy. Na základě těchto odpovědí a vzájemných souvislostí systém ZEFIS vypracuje přehled silných a slabých stránek a identifikuje klíčové nedostatky rozdělené podle zkoumaných oblastí. Tyto nedostatky jsou následně rozděleny do tří kategorií rizika: červené značící vysoké riziko, oranžové pro střední riziko a zeleně označené nízké riziko. ZEFIS dále poskytuje doporučení, jak obecně odstranit nalezené nedostatky a porovnává situaci s jinými srovnatelnými společnostmi, aby uživatelé mohli posoudit, zda se jedná o běžný problém nebo nikoliv[40].

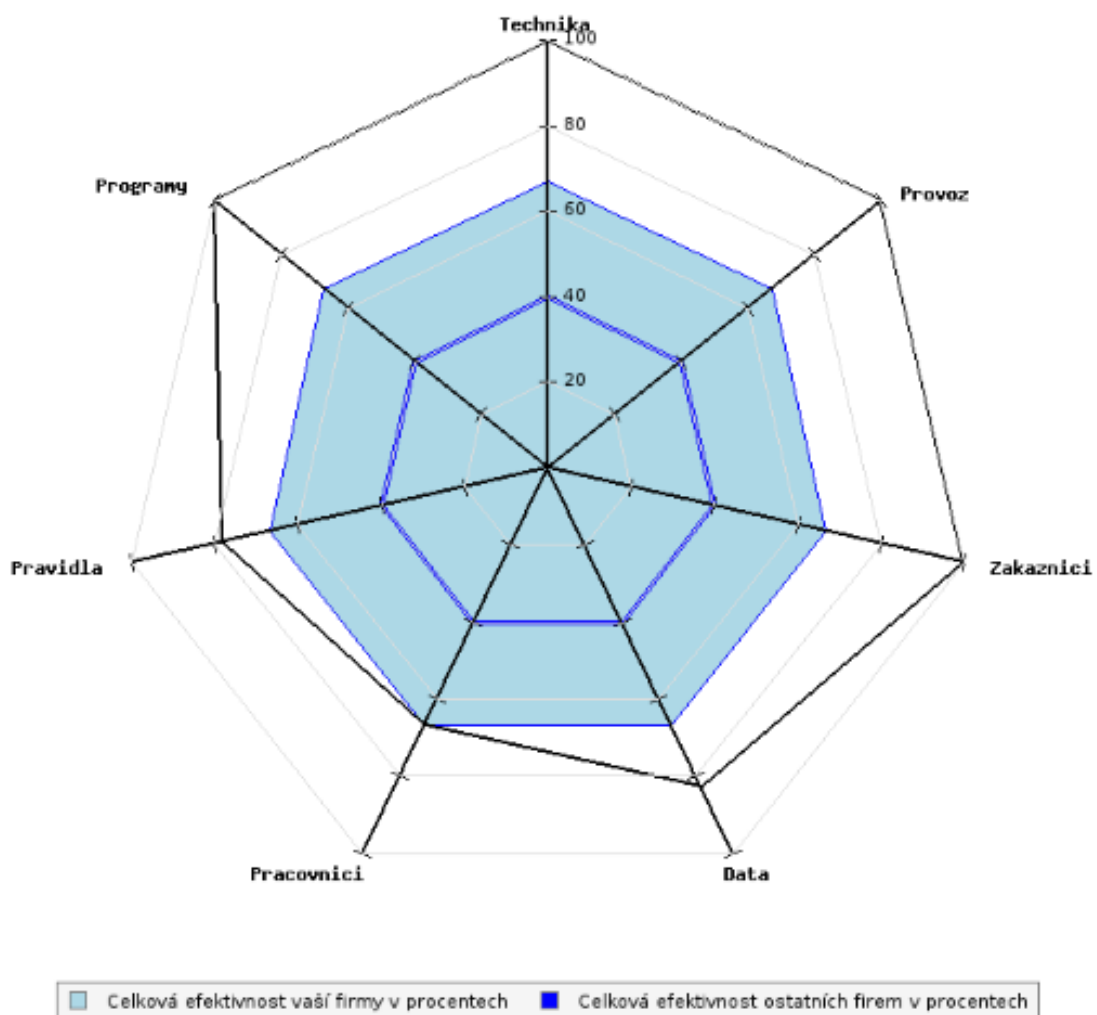
Systém hodnocení ZEFIS se zabývá riziky rozdělených do následujících sedmi oblastí:

- **Technika a hardware**

Správné technické vybavení je schopno rychle a spolehlivě realizovat požadované systémy a programy[40].

- **Programy a software**

Softwarové a programové vybavení firmy má dva hlavní úkoly: doručit správnou informaci na správné místo ve správný čas a vypomáhat pracovníkům při výkonu jejich práce[40].



Obrázek 3.8: Příklad výstupu analýzy portálem ZEFIS. Zdroj: [40].

- **Pracovníci**

Zde systém ZEFIS zkoumá, zda pracovníci jsou schopni pracovat bez chyb při dodržování stanovených pravidel[40].

- **Data**

V oblasti dat se ZEFIS zajímá o to, zda jsou bezpečně uložena, náležitě chráněna a obsahově kompletní[40].

- **Zákazníci**

U zákazníků je zkoumáno, zda daný informační systém splňuje jejich potřeby a zda jsou jejich osobní data chráněna dle vyhlášky GDPR o ochraně dat[40].

- **Pravidla a orgware**

V této oblasti systém ZEFIS dotazníky zjišťuje, zda existují náležité dokumenty k informačnímu systému – pracovní postupy, pravidla a směrnice. Zajímá se taky o jejich dodržování a kontroly[40].

- **Provoz**

Poslední oblast se věnuje podpoře zákazníků, dodržování pravidel a často řešeným problémům[40].

Systém ZEFIS je dostupný ve verzi zdarma i v placené verzi. Omezení verze zdarma oproti té licencované tkví v tom, že uživatel může analyzovat pouze jednu firmu, v ní jeden informační systém a v něm jen jeden proces. Při vyhodnocení výsledků auditu také nejsou dostupná srovnání s ostatními firmami.

### 3.9 User experience

Je těžké definovat co přesně je user experience (dále pod obecně užívanou zkratkou UX), poněvadž obsahuje řadu oblastí, jakými jsou například funkčnost, použitelnost nebo přístupnost. Pokud bychom se i tak chtěli přesné definici co nejlépe přiblížit, lze z literatury využít následující:

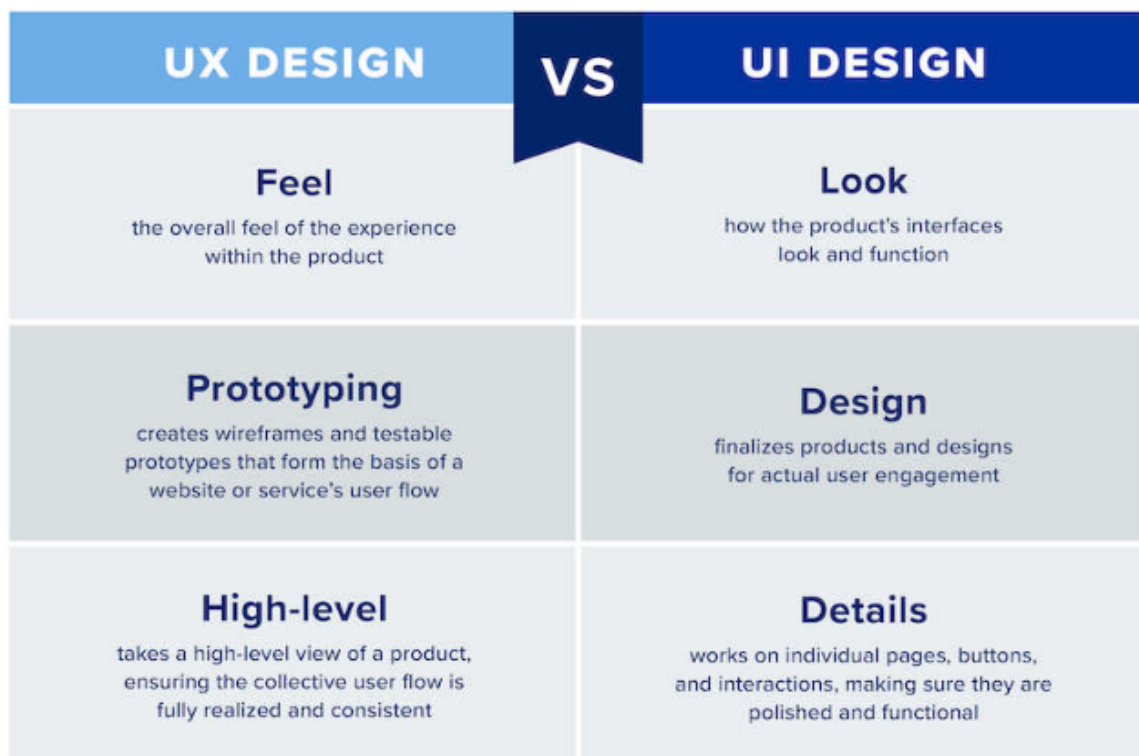
„UX design je proces designování fyzického nebo digitálního produktu, které jsou užitečné, snadno se používají a poskytují skvělou zkušenost (dojem, zážitek) při interakci s ním[3]“. Oproti souvisejícímu pojmu uživatelského rozhraní však lze zdůraznit několik klíčových rozdílů – UX se zaměřuje na celkovou zkušenost a zážitek z používání produktu, kdežto činnosti designérů uživatelských rozhraní se úzce zaměřují na vzhled. UX tvoří testovatelné prototypy, na kterých poté staví UI designéři celkový vzhled a činí jej pro uživatele vizuálně zajímavým. Posledním rozdílem je skutečnost, že UX design se věnuje tématice z vyšší úrovně abstrakce, kdežto UI design je ta oblast, která dovádí každý detail k dokonalosti. Srovnání user experience designu a user interface designu ve stručnosti zobrazuje obrázek 3.9.

### 3.10 User interface

User interface (česky uživatelské rozhraní) představuje část informačního systému, kterou vidíme, slyšíme a se kterou můžeme interagovat. Ostatní části systému jsou pro nás skryté, například databáze, kde jsou informace uloženy. I když uživatelé nevidí tyto skryté části, dokáží si do určité míry představit, jak zhruba systém uvnitř funguje. Tato představa nebo pochopení je často důležité, zejména když se uživatelé musí vypořádat se systémem, který nefunguje jak by očekávali a jsou nuceni se vypořádat s chybami[21].

Interakce se systémem probíhá pomocí uživatelského prostředí. U běžného stolního počítače se uživatelské prostředí skládá z obrazovky, klávesnice, myši a reproduktorů. V komplexnějších systémech může jít o zvukový vstup pomocí mikrofону, speciálních tlačítek a specializovaných zařízení – například MIDI ovladačů nebo grafických tabletů[21].

Informatční systémy mohou nabízet rozličná uživatelská rozhraní, která lze navíc propojovat s dalšími počítačovými systémy, jako jsou například docházkové systémy nebo elektronická pošta. Pro lepší pochopení na příkladu uveďme staré tradiční textové editory



Obrázek 3.9: Základní rozdíly mezi user experience a user interface. Zdroj: [32].

– jejich používání je komplikované a nedokázaly zpracovávat tolik dat jako současné textové editory, které jsou výrazně uživatelsky přívětivější. Zásadní rozdíl mezi starými a novými textovými editory tkví v designu uživatelského rozhraní. Ačkoli oba typy systémů plní stejnou funkci a sdílí značnou část funkcionality, jedno rozhraní je intuitivní, zatímco druhé může být vnímáno jako komplexní, které často uživateli v práci aktivně překáželo[21].

## Návrh uživatelského rozhraní

Cílem uživatelského rozhraní jsou v zásadě poměrně přímočaré – uživatel by měl být schopen v rámci svých pravomocí zobrazit a měnit data, se kterými systém pracuje. Praxe ale ukazuje, že napohled jednoduchý úkol není vůbec jednoduché realizovat. Proces tvorby takového rozhraní rozdělen na dva odlišné přístupy[21]:

- **CHI – Computer-Human Interaction**

Tento přístup připisuje prioritu počítači ve vzájemné interakci člověka a systému. Byl preferovaný v dřívějších dobách, kdy cena počítačů byla mnohem vyšší a flexibilita nižší. V současnosti již není používán a používá se opačný přístup HCI[20].

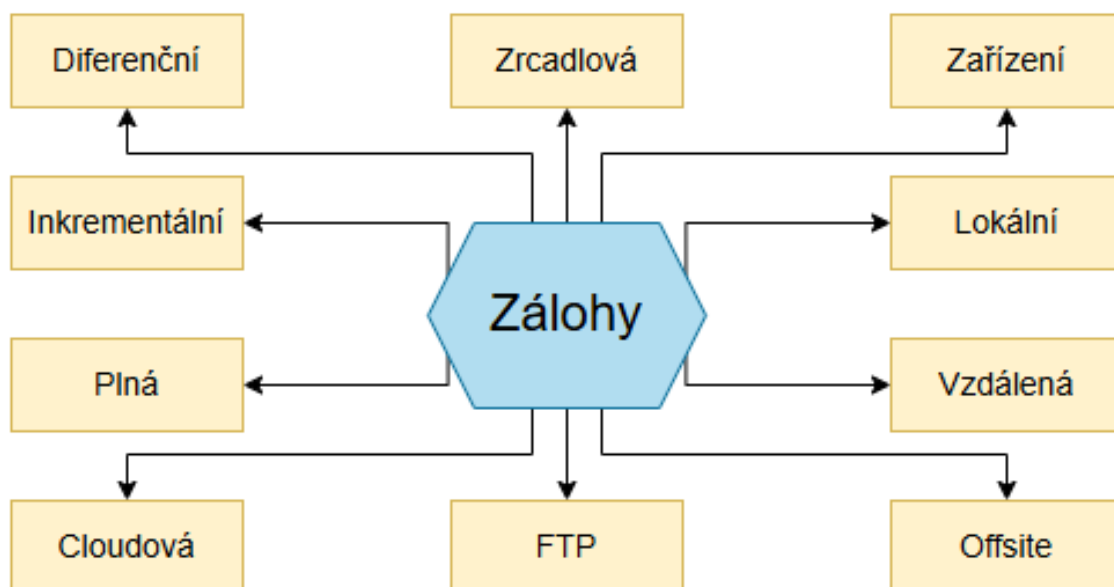
- **HCI – Human-Computer Interaction**

V současnosti výrazně více upřednostňovaný přístup HCI kladе důraz na lidskou stránku uživatelských rozhraní. Věnuje se více pohodlí uživatele, usnadnění jeho práce a vyhýbá se přílišné komplexitě. V dnešní době levných počítačů lze více

zvýšit efektivitu práce právě na straně člověka, nežli na straně samotných strojů a tak se tento přístup stal dominantní[20].

### 3.11 Zálohování

V oboru informačních technologií představuje záloha – výstup procesu zálohování dat – digitální kopii souborů, která je vytvořena a bezpečně uložena na jiném počítačovém systému, aby mohla být využita k obnovení původních dat v případě kdy dojde k jejich ztrátě. Zálohovat se dají prakticky všechny soubory, které uživatel potřebuje – například databáze s kontakty, firemními dokumenty, fotografie, videa, celé disky nebo i počítače s informačními systémy, konfiguracemi dalšími nástroji. Existuje řada přístupů a technik zálohování, přičemž každá z nich řeší různé problémy a vyhovuje různým požadavkům uživatele, viz obrázek 3.10. Před zahájením zálohování je proto nutné analyzovat a stanovit objem zálohovaných dat a za jakým účelem je zálohování prováděno[39].



Obrázek 3.10: Diagram zobrazující různé strategie při procesu zálohování dat. Zdroj: vlastní zpracování podle [39].

Následující výčet přibližuje různé typy záloh a přístupy k zálohování, které mohou jednotlivci i společnosti implementovat:

- **Plná záloha**

Plná záloha je nejčastější formou zálohy, kdy všechny potřebné soubory jsou zkopírovány na jiné úložiště. Její výhodou je jednoduchost, fakt, že celá záloha se nachází na jednom místě a rychlost obnovení dat. Naopak nevýhodou je skutečnost, že ze všech přístupů je plná záloha nejpomalejší a zabírá nejvíce diskového prostoru[39].

- **Inkrementální záloha**

Inkrementální záloha uchovává pouze provedené změny oproti předchozí záloze. Při využití takové strategie je na začátku vytvořena plná záloha a všechny následující

zaznamenávají jen data, která se změnila. Výhodou je to, že tvorba záloh je velmi rychlá, protože pouze změněné informace jsou ukládány. Díky tomu se také inkrementální přístup vyhýbá zbytečné duplikaci souborů. Naopak velkou nevýhodou inkrementální strategie je doba obnovy dat. Zde je nutno nahrát poslední plnou zálohu a pak k ní jednotlivé inkrementy přidávat, což zabere hodně času. Kvůli této vlastnosti je dobrou praxí dělat jednou za stanovené období znovu plnou zálohu, aby se uživatelé vyhlí extrémně dlouhým dobám obnovy[39].

- **Diferenční záloha**

Dá se říci, že diferenční záloha je modifikovaný pohled na inkrementální zálohu. Klíčový rozdíl tkví v tom, že inkrementální záloha uchovává změny provedené od poslední zálohy, naopak diferenční záloha uchovává změny provedené od poslední plné zálohy. Ve výsledku je tedy diferenční přístup schopen mnohem rychleji obnovovat data, protože stačí aplikovat pouze jednu zálohu od poslední plné zálohy. Naopak nevýhodou oproti inkrementální strategii je delší čas tvorby zálohy a větší nároky na úložný prostor[39].

- **Zrcadlová záloha**

Zrcadlová záloha je vytvoření přesné kopie zdrojových dat s tím, že v záloze se původní stav dat ještě nějakou dobu uchovává. Výhodou zrcadlových záloh je úspora prostoru úložiště, protože neobsahuje zbytečné a nepotřebné soubory. Velkou nevýhodou ale je, že pokud je soubor ve zdrojových datech smazán, stejný soubor je nakonec smazán i ze zrcadlové zálohy. Vzhledem k této skutečnosti by se nasazení zrcadlových záloh mělo provádět s opatrností. Omylem smazaný soubor nebo složka může uniknout pozornosti a pokud nedojde k odhalení před další zálohou, budou data ztracena jak v původních zdrojových datech, tak v záloze.

Mnoho zálohovacích služeb nabízí možnost měsíčního uchování smazaných souborů. To znamená, že když je soubor smazán na zdrojovém systému, je na úložném serveru uchován minimálně 30 dní po smazání. Tím se snižuje hrozba chyby, která může při práci se zrcadlovými zálohami nastat[39].

- **Plná záloha celého zařízení**

Úplná záloha zařízení cílí na celý počítač. Namísto pouhého kopírování dat na počítači, úplná záloha zařízení také zaznamenává stav struktury počítače. Tento obraz funguje jako snímek celého disku a může být uložen jakožto kompresovaný soubor pro ušetření prostoru. Jiné typy záloh, jenž pracují pouze s uživatelskými soubory, v případě obnovy musí programy a operační systém přeinstalovat z instalačních souborů nebo instalačního disku.

S úplnou zálohou celého počítače však může uživatel obnovit úložiště přesně do stavu, v jakém byl v době, kdy byla záloha provedena. Úplné zálohy také mají schopnost zálohovat skryté a chráněné soubory na počítači, což v praxi znamená, že uživatelé mohou uložit soubory nebo konfigurace, které by jinak mohli přehlédnout, a které jsou důležité pro provoz počítače.

Pro případy, kdy se chce uživatel pojistit proti kompletnímu selhání hardwaru je tedy tato strategie velmi dobrá, avšak váží se k ní i nedostatky. Obraz disku nemusí být kompatibilní s novým hardwarem a všechny problémy počítače v čase zálohy budou znovu replikovány i na novém zařízení. Pokud tedy zálohovaný počítač

obsahoval virus nebo trpěl jinými nedostatky, budou úplně stejně přesunuty na nový počítač[39].

- **Lokální záloha**

Lokální záloha je taková záloha, kde je úložiště umístěno ve stejné lokalitě – obvykle ve stejné budově. Tyto zálohy jsou často uloženy na dedikovaném interním nebo externím pevném disku, který je přímo připojen ke zdrojovému počítači, jenž je zálohován. Výhodou lokální zálohy je skutečnost, že je velmi snadné s její pomocí obnovit zálohovaná data, a proto dobře fungují jako ochrana před důsledky virových hrozeb, selhání hardwaru a nechtěnému mazání dat. Největší nevýhodou lokálních záloh je zranitelnost vůči přírodním katastrofám – v případě kdy dojde například k požáru budovy nebo zemětřesení, jsou spolu se zálohovaným zdrojem dat zničeny i jeho zálohy[39].

- **Offsite zálohy**

Offsite zálohy mimo premisy společnosti jsou v mnohém podobné lokálním zálohám. Rozdílem je, že offsite zálohy separují zdrojová data a zálohovaná data na různá místa. Díky tomu eliminují riziko ztráty dat v důsledku přírodních katastrof. První záloha je provedena lokálně, ale jakmile je fyzické médium (např. externí pevný disk) přeneseno na oddělené místo, stává se z ní offsite záloha. Nevýhodou offsite záloh je práce navíc spojená s přepravou úložišť a hrozba poškození dat během přenosu[39].

- **Online cloudová záloha**

Cloudová online záloha je prováděna pravidelně na vzdálené úložiště, které je připojeno k zálohovanému zařízení. V tomto případě je úložiště mimo místo uchování zdrojových dat a přes internet neustále online připojeno. Tento způsob zálohování po provedení počáteční konfigurace nevyžaduje lidský zásah pro připojení disku nebo kabelu k zálohování.

K dispozici jsou online zálohovací služby pro jednotlivce i firmy. To zahrnuje instalaci aplikace uživatelem na jejich počítač, identifikaci souborů a složek, které chtějí zálohovat, a určení času, kdy mají být zálohy spuštěny. Poté jsou data před odesláním přes internet do příslušného datového centra komprimována a šifrována.

Cloudová datová centra jsou umístěna mimo zdrojové zařízení a jsou navržena tak, aby chránila data v nich uložená před požáry a zemětřeseními, často i instalují kamerové systémy a regulují teplotu v místnostech s úložišti. Navíc mají záložní generátory v případě výpadku elektrického proudu a data jsou replikována na několika zařízeních místo jen jednoho.

Obrovskou výhodou využívání cloudových záloh je velmi vysoký stupeň ochrany proti živelným katastrofám a krádeži, vyvaruje se taky lidským faktorem způsobených chyb během procesu tvorby nebo obnovy záloh. Zároveň uchovávají data na více místech současně, což poskytuje ještě další ochranu. Nevýhodou využívání služeb cloudových úložišť je cena a doba, která je potřebná pro tvorbu nebo obnovu záloh[39].

- **Vzdálená záloha**

Vzdálená záloha je forma offsite zálohy, avšak rozdíl spočívá v tom, že uživatel disponuje přístupem k záloze přes internet a může ji obnovit prakticky odkudkoli. Výhodou oproti offsite zálohám jsou ušetřené výdaje za práci spojenou s převozem a

uchováváním záloh na odděleném místě a ještě o stupeň zvyšují ochranu proti ztrátě dat vyvolané přírodními katastrofami. Naopak nevýhodou jsou výdaje vynaložené na jejich údržbu na vzdáleném úložišti a délka trvání procesu obnovy dat[39].

- **FTP záloha**

FTP záloha se provádí prostřednictvím File Transfer Protocolu (FTP) přes internet na cílový FTP server. Tento server se obvykle nachází v datovém centru daleko od zálohovaných zdrojových dat. Protože oba způsoby mají servery umístěné na jiném místě než zdrojová data, je FTP záloha v mnoha ohledech podobná offsite záloze. Nabízí tedy prakticky stejné výhody i nevýhody, jenž jsou popsány v odstavci výše[39].

## Kapitola 4

# Analýza současného stavu

V této kapitole se práce věnuje detailnímu rozboru situace ve firmě a jeho tržním okolí. Především představuje a přibližuje vlastnosti zkoumané firmy ABC a jejího informačního systému Infosys. Dále obsahuje analýzu jejího externího okolí pomocí Porterova modelu pěti sil a pomocí rozboru PEST, Infosys je pak analyzován pomocí portálu ZEFIS. V neposlední řadě je zde blíže popsána i současná situace z pohledu informační bezpečnosti.

### 4.1 Popis analyzované společnosti

Analyzovaná společnost je v diplomové práci anonymizována a dále označována pod pseudonymem ABC. Společnost ABC působí v odvětví výroby měřicích přístrojů již několik desítek let. Jedná se o vysoce precizní a technicky velmi náročnou výrobu strojů blížící se hranici toho, co je dnešní technologie schopna vytvořit. Zaměstnává v současnosti řadu lidí, kteří se zhruba rovnoměrně rozprostírají mezi technology, administrativu a operátory výroby. Aspektům výpočetní techniky a informačních systémů se v rámci zkoumání diplomové práce věnuje pouze jeden z nich, avšak nejedná se o pozici plně dedikovanou IT infrastruktuře, nýbrž je to spíše jeho vedlejší povinnost.

Kanceláře i výroba se nachází v jedné budově, což umožňuje úzkou spolupráci mezi administrativou, designéry a operátory výroby a napomáhá sdílení znalostí mezi kolegy, což je pro úzce zaměřené strojní specialisty klíčové.

### 4.2 Popis zkoumaného informačního systému Infosys

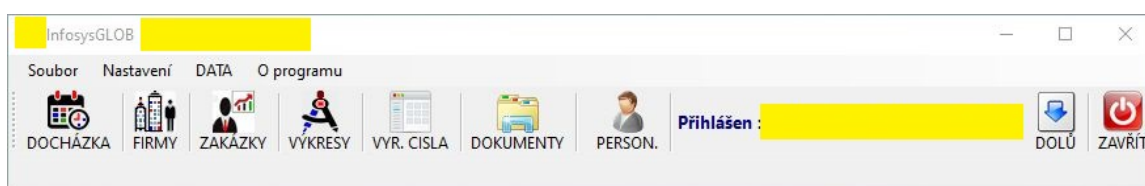
Tato diplomová práce se konkrétně zabývá posouzením informačního systému jménem Infosys, který je využíván společností ABC. Infosys je v provozu již 23 let a je schopen zpracovat většinu požadavků, které zaměstnanci ABC na informační systém mají. Jedná se o systém typu ERP, tedy *enterprise resource planning* (viz sekce o typech podnikových informačních systémech 3.4.4).

Designérem, tvůrcem i člověkem zodpovědným za další rozvoj Infosysu je jedna a ta samá osoba – bývalý zaměstnanec společnosti ABC, který jej před více než 20 lety sám interně vytvořil přímo na míru požadavkům zaměstnanců ABC. Svůj Infosys teď autor nadále prodává jako licencovaný produkt, přičemž firma ABC má dostupnou permanentní licenci a plný přístup. Tvůrce Infosysu na svém produktu stále pracuje za dohodnutou finanční odměnu, ale jedná se spíše již jen o údržbové aktivity a drobné aktualizace, nová funkcionality již není přidávána.

Vzhledem k permanentně udělené licenci k Infosysu pro společnost ABC jsou výdaje na provoz poměrně malé. Vývojář si za malé úpravy účtuje méně než 10 tisíc korun ročně a po přičtení nákladů na provoz hardwaru a pořizovací ceny zálohovacích disků činí celkové roční náklady údržby Infosysu společnost ABC méně než 30 tisíc korun ročně.

#### 4.2.1 Moduly Infosysu a jejich uživatelské rozhraní

Informační systém Infosys se skládá ze 7 modulů, jenž jsou rozděleny podle toho, kterou funkcionalitu obstarávají. Jednotlivé moduly jsou spouštěny zvlášť z tzv. *banneru*, tedy malého okna sloužícího jako vstupní bod po spuštění pro uživatele Infosysu, viz obrázek 4.1. Víceero modulů může být spuštěno najednou, což odstraňuje potřebu přepínání mezi nimi a zvyšuje množství informací, které je Infosys najednou poskytnout. Na druhou stranu se však moduly poměrně dlouho spouští a uživatelské jednoduché požadavky tím brzdí.



Obrázek 4.1: Rozcestníkový banner, který se otevře jako první okno po spuštění Infosysu. Obsahuje tlačítka v horní liště pro nastavení samotného systému a 7 dalších tlačítek pro spuštění jednotlivých modulů. Žlutě zabarvená místa zobrazují jméno přihlášeného uživatele a jméno tvůrce systému. Zdroj: vlastní zpracování.

Následující podsekcce představují všech 7 existujících modulů Infosysu a stručně popisují jejich funkcionalitu.

##### Docházka

Prvním modulem je Docházka, jenž slouží jako docházková knížka. Modul používají všichni zaměstnanci společnosti k zadávání času příchodu a odchodu z práce, k zaznamenávání doby strávené na dovolené a k přesnému specifikování toho, kolik hodin strávil zaměstnanec prací na kterých zakázkách.

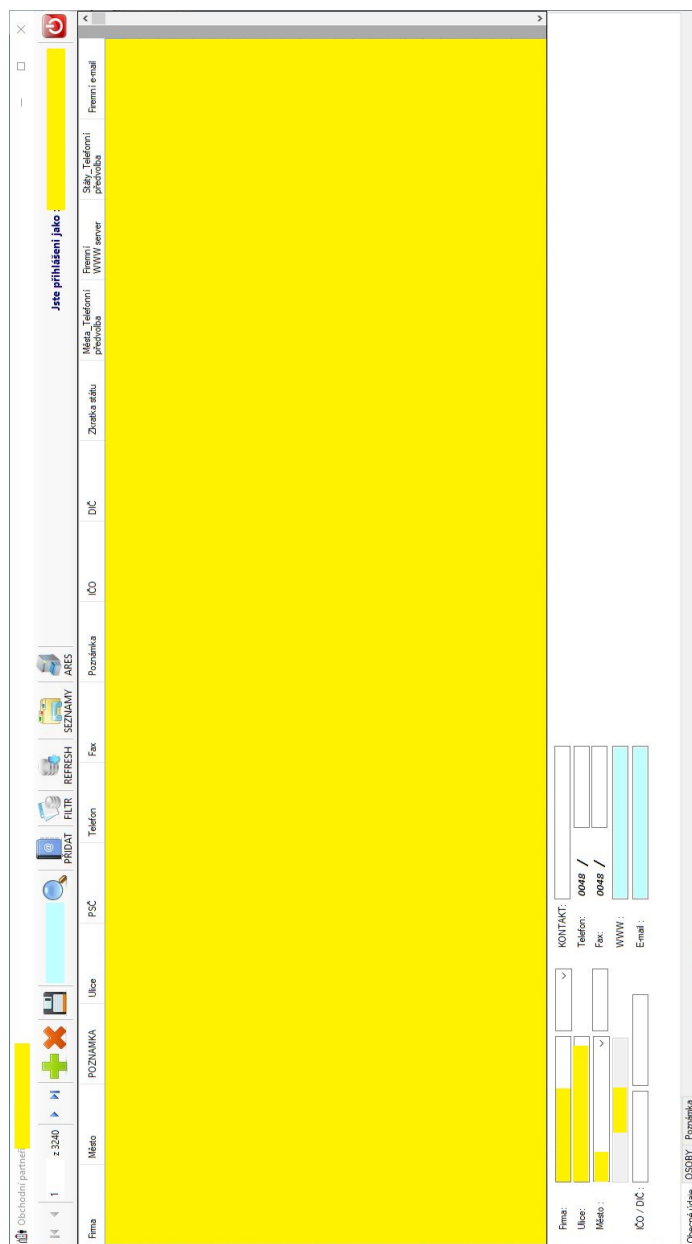
Modul umožňuje i tisk docházkových listů, viz obrázek 4.2.

##### Firmy

Druhý modul Infosysu jsou Firmy, viz obrázek 4.3. Modul zaznamenává a uchovává informace o kontaktech na osoby v cizích firmách – dodavatelích i zákaznících. Modul Firmy umožňuje úplně všem pracovníkům tvořit nové záznamy, upravovat stávající a mazat nepotřebné, dále může záznamy uživatel filtrovat, zařazovat do oddělených seznamů a aktualizovat načtenou sadu informací pro zobrazení změn provedených od spuštění modulu. Modul se dále skládá z podsekcí Osoby a Poznámky, avšak ty nejsou v současnosti využívány a místo toho jsou všechny informace zapisovány do hlavní sekce Osobní údaje.

Žádanou funkcionalitou, kterou Firmy neposkytují, je zasílání upomínek na jednání se zákazníky. V tomto ohledu jsou pracovníci nuceni použít jiných nástrojů.





Obrázek 4.3: Okno modulu Firmy. V horní liště mohou zaměstnanci přidávat, mazat, řadit, vyhledávat a kategorizovat záznamy do oddělených seznamů. Ve spodní části obrazovky mohou pracovníci upravovat již existující zvolený záznam a na spodním kraji mohou přepínat mezi podsekcemi modulu. Žlutě zabarvená místa zakrývají přehled informací o kontaktech, jméno přihlášeného uživatele a jméno tvůrce systému. Zdroj: vlastní zpracování.

## Zakázky

Třetí a nejdůležitější modul Infosysu jsou Zakázky, viz obrázek 4.4. Zakázky spojují a synchronizují dohromady ostatní moduly pomocí generovaných identifikačních čísel a vazeb mezi nimi. Oprávnění uživatelé využívají Zakázky při vnášení nově vznikajícího projektu do Infosysu, zaznamenávají informace o jeho průběhu a podle potřeby přidávají nebo upravují další záznamy o něm, jakými jsou například časový harmonogram, finanční rekapitulace nebo navázané vygenerované dokumenty. Další velmi důležitou funkcionalitou Zakázek je zobrazení seznamu všech propojených výkresů včetně několika jejich základních informací. Zakázky kromě poskytování informací o všech zakázkách, jejich zadavatelích nebo harmonogramech obsahují ještě další tři menší podmoduly:

- **Docházka + Tisky**

Podmodul obsahuje seznam lidí, kteří se na dané zakázce nějakým způsobem podílejí. U některých z nich uživatel zadává i role které zastávají, avšak u většiny z nich se tato informace nezadá, pokud není nutně potřeba. Podmodul také zobrazuje všechny napárované dokumenty k zakázce spolu se všemi případy, kdy uživatelé dokument tiskli. Záznam o tisku se však uchová jen pokud dokument tiskl uživatel pomocí funkcionality Infosysu, pokud jej tiskl zvlášť mimo systém, záznam se nevytvoří vůbec.

- **Lidi + Činnosti**

V tomto podmodulu může oprávněný uživatel zobrazovat, tvořit a upravovat informace o spolupracovnících dané zakázky a jaké činnosti plní pro její splnění. Sekce obsahuje seznam všech úkolů a jméno pracovníka či pracovníků přiřazených k jeho splnění.

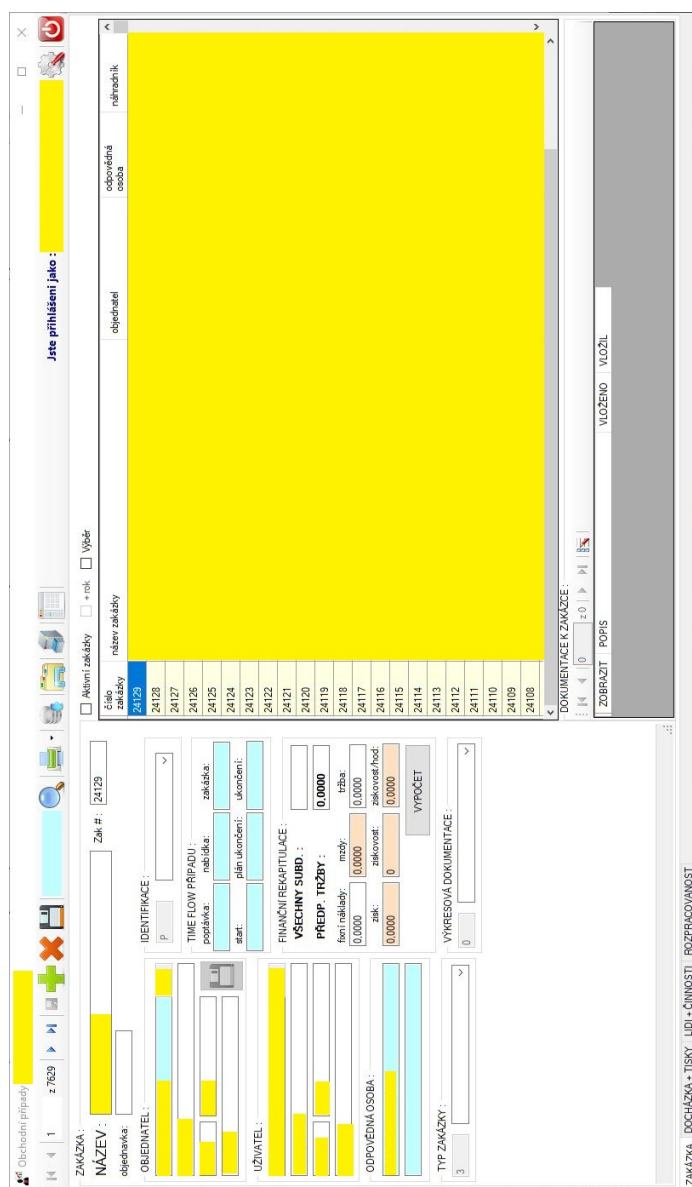
- **Rozpracovanost**

Podmodul rozpracovanost úzce souvisí s výše zmíněným Lidi + Činnosti. V této podsektci Zakázek se nachází soupis všech úkolů spolu s hodnotou, na kolik procent je úkol splněn. Informace zde, podobně jako u ostatních podmodulů, mohou vkládat, upravovat a zobrazovat pouze oprávnění uživatelé, avšak ani ti jej příliš často nevyužívají. Pro menší zakázky takové informace často nemá smysl udržovat a tak je podmodul využíván pouze pro velké projekty.

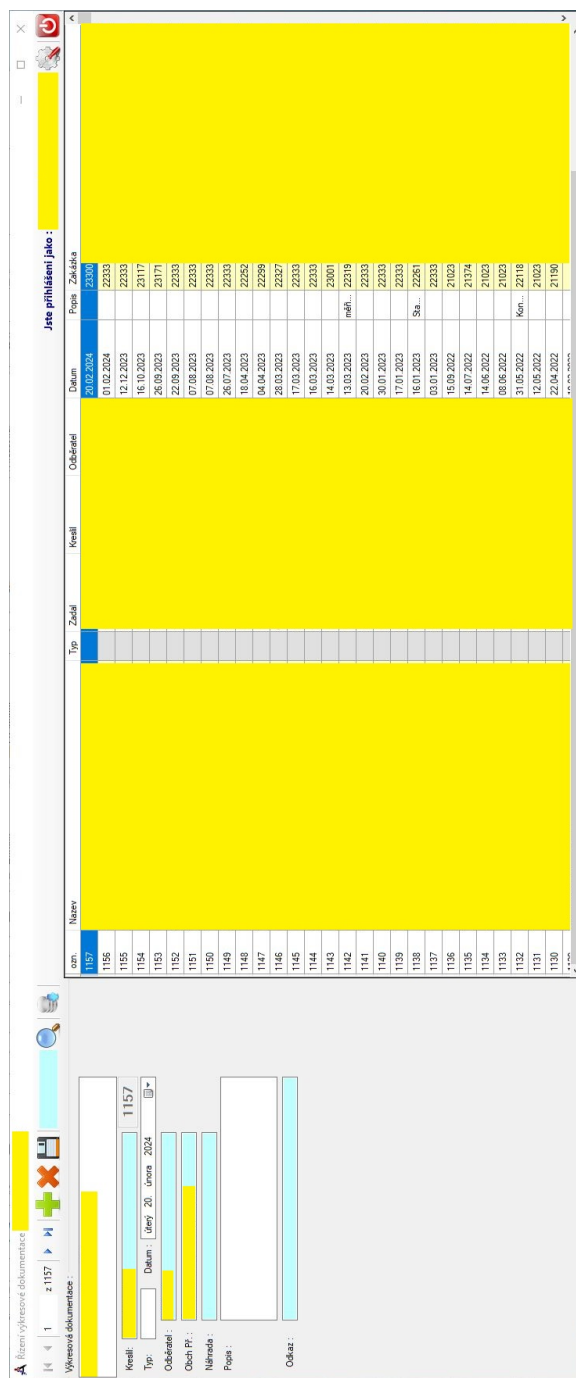
## Výkresy

Čtvrtým modulem, důležitým obzvlášť pro konstruktéry, jsou Výkresy. Modul výkresy uchovává všechny potřebné informace o konstruktérských výkresech – autora, popis, typ, zadavatele, odběratele, identifikátor přiřazené zakázky a mnoho dalšího, viz obrázek 4.5. Zároveň díky tomu, že sám generuje identifikátory výkresů, je schopen zamezit zmatkům jaké by mohly nastat v případě, kdy díly nesou velmi podobné názvy nebo lidskou chybou byly jednomu identifikátoru přiřazeno více odlišných výkresů. Modul Výkresy tedy tímto udržuje konzistenci a úplnost informací o výkresech, na jejichž základě je pak schopen správně párovat modul Zakázek.

Jedna velmi důležitá funkce ale chybí, a tou je možnost zobrazení požadovaného výkresu. Uživatel v tomto modulu tedy tvoří a upravuje pouze záznamy o výkresech, nikoliv samotné výkresy a to ani ve formě jejich exportovaných souborů. Pokud jej chce uživatel zobrazit, musí k tomu použít buďto programový nástroj ve kterém byl navrhován, nebo z něj pořízené snímky ve formě, která nevyžaduje specializovaný software.



Obrázek 4.4: Ukázka okna modulu Zakázka. V horní liště mohou zaměstnanci mimo jiné vyhledávat, procházet, tisknout nebo ukládat provedené změny. V levé polovině obrazovky se nachází textová pole, pomocí kterých může uživatel zobrazit nebo upravit detailní informace o zvolené zakázce, jejím objednavateli, odpovědné osobě, časovém plánu, finanční rekapitulaci nebo může procházet spárovanou výkresovou dokumentaci. V pravé části je vyobrazen seznam všech zakázek s několika málo základními informacemi o nich, přičemž detaily může uživatel vidět a upravovat v levé části po rozkliknutí požadovaného záznamu zakázky. Vlevo dole se pak nachází tlačítka sloužící k přepínání mezi podmoduly a vpravo dole seznam všech vytvořených dokumentů, které jsou spojeny s danou zakázkou. Žlutě zabarvená místa zakrývají názvy a další informace z přehledu zakázek vpravo, detailní záznamy o zvolené zakázce v levé části, jméno přihlášeného uživatele a jméno tvůrce systému. Zdroj: vlastní zpracování.



Obrázek 4.5: Ukázka obrazovky modulu Výkresy. V horní liště může oprávněný uživatel procházet, přidávat, mazat či hledat požadovaný výkres. V levé části obrazovky se nachází detailní informace o konkrétním výkresu, jakými jsou například název, autor, typ, popis a další. V pravé části okna modulu se pak zobrazuje kompletní list všech existujících výkresů s několika málo nejdůležitějšími informacemi o něm – pro zobrazení či úpravu všech detailních informací stačí výkres v pravém okně označit a informace vlevo podle vůle upravit a uložit. Žlutě zabarvená místa zakrývají názvy a další informace z přehledu výkresů vpravo, detaily zvoleného výkresu v levé části, jméno přihlášeného uživatele a jméno tvůrce systému. Zdroj: vlastní zpracování.

## Výrobní čísla

Pátým modulem jsou Výrobní čísla – modul používán především konstruktéry. Infosys za pomoci Výrobních čísel předchází potenciálním zmatkům ve výrobě a údržbě dokumentace a zároveň uchovává celkový přehled o existujících již použitých číslech. Narozdíl od všech ostatních modulů pracují Výrobní čísla ve třech různých oknech, z nichž každé poskytuje jinou funkcionalitu. Každému z nich se blíže věnuje následující výčet:

- **Výrobní zakázky**

Okno výrobních zakázek umožňuje uživateli zobrazit část informací o výrobku na základě poskytnutého výrobního čísla (viz obrázek 4.6). Uživateli je po jeho zadání zobrazeno jméno autora, přiřazená zakázka, účel dílu a identifikační číslo jeho výkresu. Uživatel je pak také schopen zjistit kdo, jak dlouho a jakou činnost s dílem prováděl a sám také podobné záznamy tvořit. Informace zadány v tomto podmodulu jsou pak využity v jiných podmodulech (oknech) modulu Výrobní zakázky.

- **Výrobní objednávky a výroba dílů**

Druhým a funkcionalitou zdaleka největším podmodulem je Výrobní objednávky a výroba dílů. Zde se podmodul dělí na dvě následující části, viz obrázek 4.7.

První část *Výrobní čísla - SÉRIOVÁ* dohromady kombinuje existující zakázky, objednávky a výkresovou dokumentaci spolu s termíny, popisem a zodpovědnými osobami do společné vazby výrobní objednávky. Oprávnění uživatelé pak podmodul mohou využít k tvorbě nových, úpravě stávajících nebo odstranění záznamů výrobních objednávek.

Druhá část *Výroba dílů* pracuje s informacemi o jednotlivých instancích, kdy byl vyroben jeden nebo více dílů toho samého typu. Podmodul k existujícímu výkresu přiřadí popis, počet vyrobených kusů, termín a uchovává jeho současný stav. Dále je schopen pracovat i s parametry vazby na danou zakázku, zodpovědnými lidmi prováděné činnosti nebo externí náklady, avšak tato funkcionalita není v praxi vůbec využívána kvůli zbytečné pracnosti, která nepřináší opodstatněnou přidanou hodnotu.

- **Řízení výrobních čísel**

Podmodul Řízení výrobních čísel se věnuje tvoření, zobrazování a modifikování záznamů o jednotlivých vygenerovaných výrobních číslech. Oprávnění uživatelé zde mohou procházet existující čísla, zobrazovat či upravovat informace o nich nebo tvořit úplně nové záznamy, viz obrázek 4.8. Obsahuje mimo ty základních i informace o objednavateli, vazby na zakázku, výkresy, zodpovědnou osobu nebo typ dílu.

výrobní zakázky

odhlášení: 38 s

**Zakázka:**

Jméno: .....

Činnost: .....

Výkres: .....

VLOŽ KÓD

Vstup dat:

pondělí 15. dubna 2024

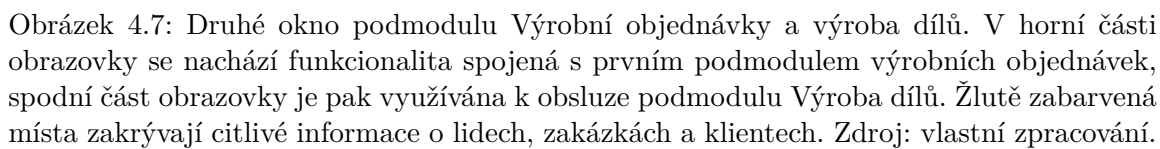
Čas: .....

VLOŽ DATA

Stavba zakázek a nákladů pro výroby výkres:

| JMÉNO | Činnost | Čas | zakázka |
|-------|---------|-----|---------|
|       |         |     |         |

Obrázek 4.6: První okno podmodulu Výrobních zakázek. V levé horní části jsou po zadání požadovaného kódu dílu zobrazeny základní informace o něm a v levé dolní části se nachází výpis lidí kteří se na něm podíleli, jakou činností a jak dlouho. Žlutá místa zakrývají skutečný název firmy ABC a jméno přihlášeného uživatele. Zdroj: vlastní zpracování.





## Dokumenty

Šestý všem dostupný modul se nazývá Dokumenty, avšak slouží především administrativním a vedoucím pracovníkům. Hlavním cílem Dokumentů je správa vzorů a tisku dokumentů. Uživatel zde může vybrat jeden z existujících vzorů, zadat potřebné informace a obdrží vygenerovaný soubor s vyplněnými poskytnutými informacemi. Modul Dokumenty také umožňuje zobrazit již vytvořené dokumenty, a to i dokumenty vytvořené jinými uživateli (kromě nabídek). Nad jejich seznamem pak mohou pracovníci pracovat s filtry a řazením, viz obrázek 4.9.

Modul Dokumenty je schopen vytisknout dohromady 14 různých typů:

- *Objednávka*: Šablona dokumentu zachycující specifikace objednávky od zákazníka. Obsahuje informace o zákazníkovi, datu tvorby objednávky, očekávaný časový harmonogram a popis spolu s výčtem požadovaných kusů. Dokument je využíván v případech, kdy zákazník již přesně ví, které stroje a služby od společnosti ABC potřebuje.
- *Dodací listy*: Často využívaný záznam o dodání produktu zákazníkovi nebo o obdržení výrobních vstupů od dodavatele. Obsahuje datum předání a výčet zakoupeného či prodaného zboží. Jedná se o jeden z nejčastěji používaných dokumentů.
- *Dopis*: Vzory dopisů rozesílaných obchodním partnerům. Dříve byly využívány často, postupně ale jejich použití s nástupem elektronické komunikace klesalo. Dnes se kromě upomínek jiné typy dopisů používají jen zřídka.
- *Fax*: Vzor pro fax, dříve zřídka ale v současnosti není už vůbec využíván.
- *Kalkulace*: Dokument obsahující informace o výpočtu ceny pro konkrétního zákazníka. Obsahuje informace o nabídce, konkrétní částku očekávaných nákladů a návrh ceny pro koncového zákazníka. Kalkulace se ale v současnosti ve společnosti ABC řeší již plně online a tento dokument není využíván.
- *Nabídka*: Důležitý a poměrně často využívaný vzor dokumentu, který obsahuje informace o nabídce společnosti ABC pro své zákazníky. Obsahuje přesné informace o nabízeném produktu, době dodání, požadované částce a další smluvní dodatky. V minulosti byla pravomoc zobrazovat tyto velmi citlivé informace zneužita a v současnosti uživatelé potřebují zvláštní oprávnění pro přistupování k tomuto typu dokumentů.
- *Opatření*: Dokument popisující zavedená nebo nově zaváděná opatření. Dříve se občas používal pro tisk nových bezpečnostních opatření do výroby, avšak v posledních letech jej nikdo nevyužívá.
- *Poptávka*: Vzor obsahuje informace o cílové dodavatelské firmě, od které ABC požaduje dodání vstupu pro svoji další činnost. Může se jednat například o součástky do nově vznikajících strojů, avšak v současnosti se dokument nepoužívá a místo něj se používají jiné způsoby poptávání zboží.
- *Předávací protokol*: Protokol obsahující informace o datu, typech, množstvích a kvalitách předávaného zboží. Je používán jednak pro styk mezi společností ABC a jejími dodavateli, ale i pro zákaznický styk. Narozdíl od dodacího listu obsahuje více informací o stavu zboží, jeho stáří a podmínkách ve kterých fungoval.

- *Servis*: Vzor dokumentu s informacemi o zákaznickém servisu produktů poskytnutých společností ABC – jeho počátečním a koncovým datem, délce trvání, provedené práci a seznamem pracovníků podílejících se na servisu.
- *Výstupní kontrola*: Dokument obsahující popis produktu, datum kontroly a výčet provedených měření. U každého měření je zaznamenáno zda splňuje očekávání a u některých z nich jsou uvedeny i konkrétní naměřené hodnoty, avšak v posledních letech je dokument výstupní kontroly využíván zřídka.
- *Zadání*: Dokument popisující zadání úkolu pro zaměstnance. Obsahuje informace o úkolovaném pracovníkovi, zadavateli, předpokládaný časový harmonogram, popis samotného úkolu a očekávaný výstup, někdy v podobě akceptačních kritérií. Bohužel kvůli rozsáhlosti požadovaných informací a často zbytečných časových nákladů spojených s byrokracií zaměstnanci ABC touto formou úkoly nezadávají a místo toho používají jiné metody.
- *Zápis*: Další často využívaný dokument je zápis z interní porady nebo z jednání s externími firmami. Obsahuje záznamy o tom kdy porada proběhla, kdo se zúčastnil, agendu porady a z ní vyvozené závěry spolu s dalšími relevantními poznámkami a informacemi.
- *Způsobilost+shoda*: Dokument o způsobilosti a shodě slouží jako certifikát o splnění legislativou udávaných podmínek a parametrů. Vydává jej podnik ABC spolu s prodaným produktem a popisem, jaké právní normy splňuje. Slouží pak i jako důležitý dokument pro zákazníka například pro případ kdy u něj bude probíhat auditní prohlídka.

## Persons

Poslední sedmý modul se nazývá Persons, viz 4.10. Tento modul může být používán všemi vedoucími pracovníky, což vzhledem k povaze citlivých osobních informací není dobrý stav. Modul totiž umožňuje tvořit, mazat a zobrazovat záznamy o současných i bývalých zaměstnancích, z nichž každý záznam obsahuje citlivé informace od data a místa narození, přes adresu bydliště až po pojišťovnu a plat.

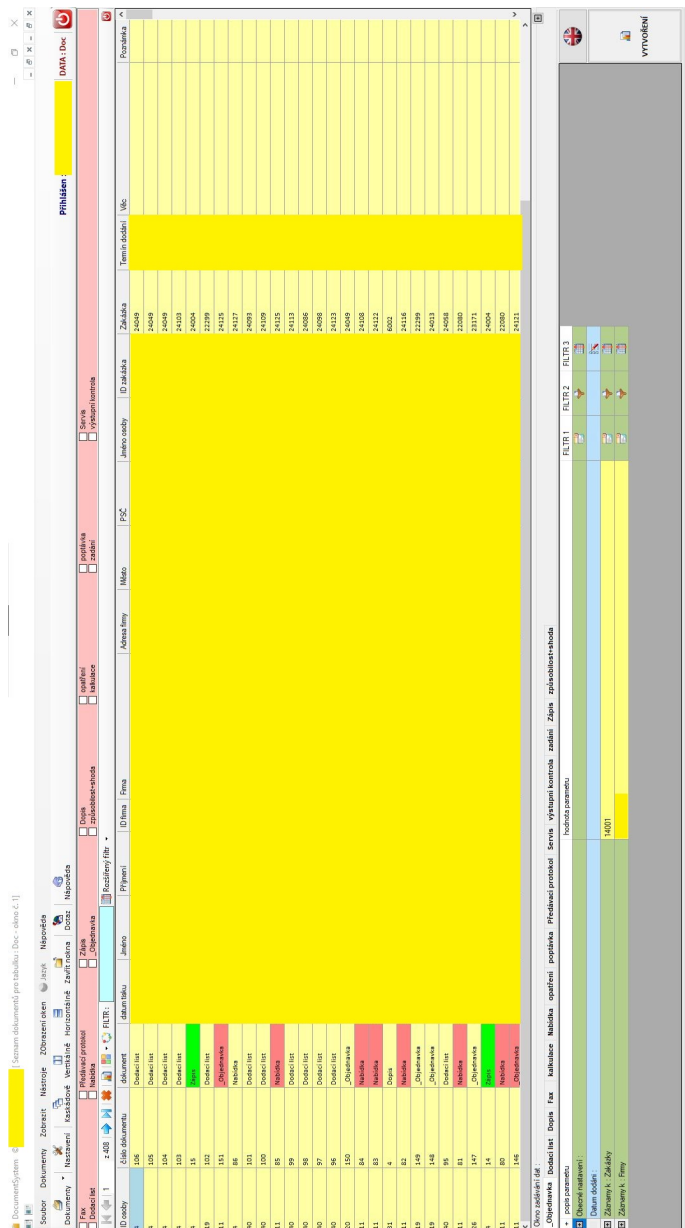
V praxi jej ale management využívá spíše pro správu hesel, přiřazení emailové adresy a kalkulace nákladů za hodinu práce jednotlivých pracovníků. I tak ale poměrně snadná dostupnost informací takové povahy může představovat bezpečnostní riziko.

### 4.2.2 Technické specifikace Infosysu

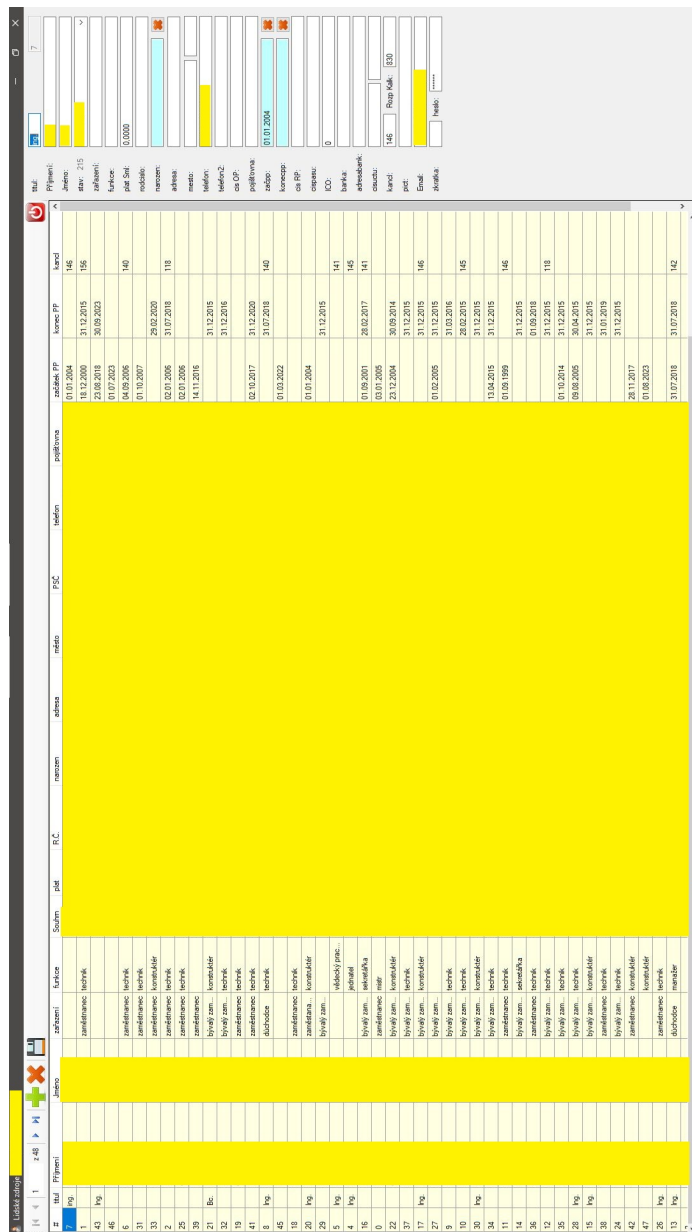
Následující sekce se věnuje posuzovanému Infosysu z technického pohledu a pohledu jeho samotné implementace – nástrojům použitých během jeho vývoje, hardwarovým prostředkům které slouží jako jeho nositelé a o technologiím, na kterých informační systém staví.

#### Platforma pro běh Infosysu

Infosys je uživateli spouštěn jako spustitelný .EXE soubor, čímž se poměrně silně váže na operační systémy Windows. Jeho spuštění na UNIXových systémech je sice teoreticky možné použitím programového nástroje *Wine*[38], avšak takový přístup je dále ztěžován tou



Obrázek 4.9: Okno modulu Dokumenty se skládá ze tří částí – vrchní části, kde uživatel může nastavovat způsob zobrazení a filtrování již existujících dokumentů například podle názvu, typu nebo autora. Prostřední část obrazovky zabírá prostor pro samotné zobrazení požadovaných informací, tedy listu vytvořených dokumentů a jejich attributech. Zobrazují se informace jako datum vzniku, číslo dokumentu, jméno autora, číslo zakázky nebo adresovaná firma. Ve spodní části obrazovky je uživatel schopen vytvořit dokument nový – vybere pomocí záložek lišty požadovaný typ dokumentu, vyplní náležitě informace, zvolí jazyk dokumentu a po stisknutí tlačítka VYTVOŘENÍ Infosys vygeneruje úplně nový dokument s unikátním číslem. Žlutě zbarvená místa zakrývají přehled dokumentů, jméno přihlášeného uživatele a jméno tvůrce systému. Zdroj: vlastní zpracování.



Obrázek 4.10: Ukázka okna modulu Persons. V horní liště mohou vedoucí zaměstnanci přidávat a mazat jednotlivé záznamy, v pravé části obrazovky se nachází sekce umožňující úpravy existujících záznamů. Prostřední část pak zobrazuje samotná data o všech současných i bývalých zaměstnancích. Žlutě zabarvená místa zakrývají přehled osobních informací, jméno přihlášeného uživatele a jméno tvůrce systému. Zdroj: vlastní zpracování.

skutečností, že data Infosysu jsou ukládána a zpracovávána v adresářích sdílených disků a zajistit kompatibilitu mezi postupy práce se souborovými moduly operačních systémů je poměrně obtížný úkol. Infosys je vyvíjen a udržován jedním člověkem a jeho použitelnost na jiných platformách než je Windows nikdy nebyla požadována, což z jeho migrace nebo nasazení s použitím jiných operačních systémů činí velmi obtížný, až nemožný úkol.

### **Oprávnění pracovníků k užívání Infosysu**

Nový uživatel Infosysu nemá správně od začátku přístup vůbec nikam. Aby mohl začít využívat alespoň podmnožinu jeho funkcionality, je nutné aby mu byla přidělena hlavním administrátorem náležitá oprávnění. Správce pak musí v průzkumníku souborů systému Windows najít na sdílených discích odpovídající složku a udělit oprávnění novému uživateli pro práci s tímto adresářem. Uživatel pak bude moci alespoň nahlížet do dat obsažených v příslušném modulu.

Přístupová práva se přidělují na základě principu need-to-know, tedy pracovníkům se udělují jen taková práva, která nutně potřebují ke své práci. Neexistuje však žádný způsob, jak hromadně práva přidávat nebo odebírat – jedinou možností je manuální nastavování každého z nich zvlášť pro každého uživatele.

### **Nástroje využívané k implementaci**

Programovacím jazykem zvoleným k implementaci Infosysu je C/C++[6]. Ten tvoří pevné a léty ověřené základy celého systému, který dále rozšiřuje framework Qt[27]. Právě Qt dodává jazyku C++ schopnosti a funkcionalitu potřebnou k tvorbě desktopových aplikací a jejich uživatelského rozhraní spolu s dalšími nástroji usnadňujícími vývoj softwaru, jako například testovací framework a optimalizační analyzátoři.

Samotná data obsažená v Infosysu jsou pak uloženy buď v programu Microsoft Access[23], nebo ve zvláštních složkách na sdílených discích. Textová data, jakými jsou například jména, adresy zákazníků, data dodání nebo osobní údaje zaměstnanců, jsou uchovávána v prostředí aplikace MS Access. Vygenerované dokumenty, výkresy nebo vzory dokumentů jsou pak uchovávány ve složkách zvlášť oddělených od běžně využívaných adresářů.

### **Nasazování a archivace verzí**

Verzování Infosysu probíhá manuálně s přičiněním správce systému. Verzování systému je velmi důležitým procesem v průběhu jeho vývoje a životního cyklu – tvůrci softwaru by měli vydávat jednou za časové období jeho verze, tedy takový stav programu, ve kterém je stabilní, spolehlivý a bez žádné rozpracované funkcionality. V případě, že se pak během dalšího vývoje stav programu zhorší a již nebude fungovat dle očekávání, mohou se vývojáři vrátit zpět k záchrannému bodu, tedy poslední verze programu. Právě toto má na starosti správce systému a jeho vývojář – administrátor uchovává jednotlivé verze spustitelných .EXE souborů a mezitím vývojář pracuje a jedenkrát za rok vydá verzi novou, která je pak otestována, nasazena a stávající verze archivována na jednom z firemních sdílených disků pro případ, kdy by vznikly problémy kvůli verzi nové. Uchovávány jsou pouze již zkompileované spustitelné soubory, přístup ke zdrojovým kódům má pouze hlavní vývojář.

### **Zálohování dat Infosysu**

Proces zálohování dat je klíčová součást informační bezpečnosti. Při zálohování tvoří odpovědná osoba kopie dat a ty pak přesouvá na jiné hardwarové úložiště pro případ, kdy

stávající médium selže. V případě kdy se společnost chce chránit i před riziky živelných katastrof nebo požárů v budovách, měly by úložiště záloh být i fyzicky odděleny v dostatečné vzdálenosti od serveru kde je s nimi nakládáno.

Společnost ABC se k zálohování dat staví zodpovědně a nebere riziko selhání hardwarového úložiště či škod v budově na lehkou váhu. Odpovědná osoba za celý proces je správce systému Infosys – ten jednou za rok vytvoří kopie databází textových dat uložených v MS Access, jednou měsíčně zálohuje vygenerované dokumenty na zvláštní archivační sdílený disk a dvakrát ročně všechna data nakopíruje na nově zakoupené pevné disky a uskladní na bezpečném místě několik desítek kilometrů daleko.

### **Síťová bezpečnost Infosysu**

Infosys není hostován na konkrétním serveru otevřenému internetu, nýbrž se jedná spíše o řadu distribuovaných síťových sdílených disků, nad nimiž operuje Infosys desktopová aplikace. Z toho důvodu nelze manipulovat se systémem mimo lokální síť sídla společnosti ABC, což eliminuje celou řadu rizik spojených s přístupností firemních dat z internetu, odpadá nutnost tvorby demilitarizovaných zón a komplexních firewall konfigurací. Namísto toho řeší svou bezpečnost pomocí externí firmy, která jedenkrát za rok provede update routeru spolu s jeho bezpečnostními politikami a nastavením.

Na druhou stranu je izolace od internetu nevýhodou pro zaměstnance v případě, kdy chtějí pracovat z domu. Infosys pracuje pouze v rámci své lokální sítě v kanceláři a v případě pokud s ním chce interagovat pracovník mimo kancelář, udržuje správce IT virtuální privátní síť – VPN (Virtual Private Network). Právě VPN umožňuje obcházet fyzické limitace lokálních sítí pomocí tvorby šifrovaných síťových toků paketů operujících i na nezabezpečených veřejných sítích. Zaměstnanec se tak při práci z domu může připojit do VPN a pracovat s Infosysem stejným způsobem, jako by byl osobně přítomen v kanceláři.

## **4.3 Porterova analýza pěti sil**

Porterova analýza pěti sil se věnuje rozboru okolí firmy a jejich vnějších vlivů, zejména vlivu konkurence, dodavatelů a zákazníků. V následující sekci jsou zmíněné vlivy podrobněji popsány a analyzovány.

### **Vliv zákazníků**

Jednací síla zákazníků vůči výrobcům je obrovská, zákazník si v podstatě diktuje co přesně, kolik strojů a pro koho bude vyrobeno. Zákazník totiž za výrobcem přijde se svým konkrétním problémem, pro který výrobce navrhne a vytvoří specifické řešení na míru pro něj. Měřicí stroje se totiž nevyrábí hromadně, nýbrž prakticky vždy podle konkrétních specifikací zákazníka. V případě kdy firma ztratí svého odběratele, je to pro ni citelná rána, čímž dává do rukou klienta obrovskou sílu a vliv na trh.

### **Vliv dodavatelů**

Síla dodavatelů vůči společností zabývajících se výrobou měřicí techniky je skoro až zanedbatelná. Materiály pro tvorbu šasi jsou levné a hojně dostupné prakticky po celém světě a i sofistikovanější komponenty jako kamery či snímače jsou k dostání od širokého spektra dodavatelů. Ač všichni z výrobců nejsou schopni uspokojit poptávku těch

nejkvalitnějších součástí, pořád jich je příliš mnoho na to, aby to mohlo ohrozit výrobní proces. Pokud by se stalo, že výrobci strojů vypadne dodavatel nebo jsou nespokojeni s jeho produkty, mají i tak na výběr mnoho alternativních poskytovatelů. Ve vztahu k dodavateli je tedy síla jednoznačně na straně zákazníka – výrobce samotného stroje.

## **Existující konkurence**

Konkurence na trhu výrobců měřicích a kontrolních přístrojů není příliš vysoká, poněvadž se jedná o poměrně specifický a úzce zaměřený trh. Strategii tohoto tržního sektoru lze v zásadě rozdělit na tři rozdílné přístupy. Tím prvním je výroba nízkonákladových strojů, které se věnují spíše validaci součástí, než jejich precizním zkoumáním a rozbořem. Takové firmy nejsou přímým konkurentem, protože jejich výrobky plní o trochu jinou funkci, nežli produkty společnosti ABC. Druhým přístupem je výroba drahých, zato vysoce kvalitních a přesných strojů. V Evropě se takové firmy nachází například v Německu, Francii či Švédsku, avšak jejich počet a celkový objem výroby netvoří tvrdé konkurenční prostředí. Třetím typem konkurence jsou společnosti primárně se zaměřující na proces automatizace výroby svých zákazníků. Takové společnosti obecně nejsou schopny dodat měřicí techniku v takové kvalitě jako ABC, své zákazníky si ale získávají právě díky jejich schopnosti automatizovanou výrobu celou navrhnout, zhotovit a implementovat bez potřeby vstupu dalších dodavatelů.

## **Hrozba vstupu nové konkurence na trh**

Bariéra vstupu na trh v odvětví měřicích přístrojů je vysoká a vytvořit novou, konkurenceschopnou společnost není jednoduché. Firmám v tom brání hlavně tyto skutečnosti:

- **Potřebná technologie a know-how**

Designérů takto vysoce sofistikovaných přístrojů je na trhu práce málo a know-how jak takové stroje vyrábět se z velké části tvoří předáváním a tvorbou nových znalostí. Společnost musí přesně porozumět požadavkům zákazníka, být pro jeho problém schopna vymyslet řešení na míru a nově navržený stroj postavit, což vyžaduje široké spektrum znalostí a zkušeností.

- **Náklady na pořízení součástí**

Obecně se dá říct, že měřicí přístroje se skládají z levných materiálů pro tvorbu šasi a z měřicích snímačů. Právě tyto snímače, kamery, detektory a další technologicky náročné komponenty musí dosahovat vysoké kvality a spolehlivosti, čemuž odpovídá výše nákladů k jejich koupi. Nově vzniklá společnost tedy musí disponovat dostatečně velkým kapitálem, aby byla schopna si jejich pořízení dovolit.

- **Náklady na sestavení produktu**

Manuální práce potřebná ke kompletaci nového měřicího přístroje je také poměrně drahá, poněvadž vyžaduje důkladně vyškolenou pracovní sílu a zaměstnance s citem pro detail. Na trhu se takových pracovníků nevyskytuje mnoho a k plnění jejich úkonů je třeba řada školení a trpělivosti, což dále navyšuje výrobní náklady.

- **Potřeba softwaru na míru pro každý stroj**

Každý typ měřicího přístroje splňuje požadavky specifické právě pro něj a skládá se z komponentů, které se od jiných typů liší. Pochopitelně tedy nelze vytvořit jediný krabicový software, který je schopen fungovat na všech strojích pro všechny účely, ale vyvíjet specifické moduly a funkcionalitu na míru. Tady má nově vznikající firma možnost buď najmout několik softwarových inženýrů a několik měsíců si jej vyrábět sama, nebo si draze zaplatit externí firmu, která to za ni udělá za mnohem kratší dobu bez potřeby zaměstnávat programátory. V obou případech ale firma spotřebuje velké množství zdrojů.

Všechny výše zmíněné faktory sice výrazně snižují riziko vstupu úplně nového konkurenta na trh, avšak pořád zůstává hrozba situace, kdy zaměstnanci firmy ABC se rozhodnou své zaměstnání opustit a vytvořit svoji vlastní firmu ve stejném oboru. Takový případ pro ABC znamená nejen vznik nové přímé konkurence, zároveň také úbytek pracovníků s jejich znalostmi a vyšší poptávku na pracovním trhu po odbornících v dané problematice.

## **Hrozba substitutů**

Pokud se rozdhlédneme na trhu po substitutech kontrolních přístrojů, nalezneme manuální lidskou práci a univerzální 3D měřicí přístroje. V případě, že se konzument měřicích přístrojů rozhodne využít lidské práce, narazí na několik problémů:

- **Nízká efektivita**

Každý stroj je několikanásobně rychlejší, než je jeho lidský protějšek, k nahrazení každého stroje je tedy potřeba několik lidí. Stroj je navíc schopen pracovat prakticky nepřetržitě narozdíl od lidských protějšků, což dále zvyšuje počet lidí a náklady potřebné k nahrazení měřicího přístroje.

- **Nízká spolehlivost**

Ač ani přístroje neměří s dokonalou přesností, stále odvádí nesrovnatelně spolehlivější výkony nežli lidé. Chyba lidského faktoru zde tvoří velké riziko, které může mít vážný dopad jak na společnosti níže na výrobním řetězci, tak na společnost samotnou.

- **Potřeba většího prostoru pro práci**

Každý pracovník by pro svůj výkon potřeboval své vlastní pracovní místo s dobrým osvětlením a svými vlastními nástroji, které zabírají cenný prostor ve výrobní hale a tím snižují efektivitu jeho využití. A ač je mnohem snadnější přestěhovat pracovní místo lidského pracovníka, nevyváží to nevýhodu neefektivního využití místa ve výrobě.

- **Náklady na lidské zdroje**

Lidský substitut měřicího stroje navíc vyžaduje náklady navíc spojené s pojištěním, zaměstnaneckými benefity a další prací pro management. Dalším faktorem v neprospěch lidských pracovníků je bezpečnost práce a ochrana zdraví, které s sebou nesou řadu dalších nákladů a zodpovědnosti.

Z výše zmíněných důvodů lidská práce není dostatečně dobrým dlouhodobým substitutem. Stále existuje další alternativa, a tou je nasazení výše zmíněných 3D univerzálních měřicích přístrojů. Takové stroje mají řadu výhod i nevýhod, přičemž v našem kontextu jsou pro nás relevantní hlavně následující vlastnosti:

- **Flexibilita**

Obrovskou výhodou univerzálních přístrojů je jejich flexibilita – pomocí správného softwaru jsou schopny zjistit více metrik, více typů součástek a využít k tomu širší výběr měřicích technik. Tímto se stávají pro řadu firem preferovanou alternativou v případech, kdy vyrábí mnoho rozličných dílů a nemohou si dovolit spravovat velký počet specifických přístrojů pro každý z nich.

- **Rychlost měření**

Ač jsou univerzální 3D stroje schopnější širší škály úkonů, znamená to také, že nijak zvlášť neexcelují ani v jednom z nich. Metriku, kterou získá řádově během desítek sekund, jsou schopny specificky navržené měřicí stroje získat během několika málo vteřin, což z univerzálních 3D strojů činí v tomto ohledu několikanásobně méně efektivní alternativu. Pokud jde výrobci součástek primárně o rychlost s jakou měřicí přístroj operuje, pak nejsou univerzální 3D stroje ideální volbou.

- **Cena**

Důležitým rozdílem mezi 3D stroji a specifickými měřicími zařízeními je pak jejich pořizovací cena. Pořizovací náklady flexibilnějšího 3D přístroje jsou velmi vysoké, což činí pokusy o sestavení výrobní linky pouze s nimi znatelně dražší oproti případu, kdy jsou do linky zavedeny specifické měřicí stroje.

Z analýzy substitutů vyplývá, že pro firmy vyrábějící rozmanité díly s rozličnými parametry kde je důležitá flexibilita procesu jsou často lepší volbou univerzálnější 3D stroje, avšak pokud se výrobce součástek věnuje užšímu spektru produktů jichž vyrábí větší počet, jako vhodnější řešení se nabízí specificky zaměřené přístroje společnosti ABC.

## 4.4 PEST analýza

Tato kapitola obsahuje analýzu vnějšího makrookolí PEST společnosti ABC. Analýza se zaměřuje na čtyři faktory: politické a legislativní, ekonomické, sociální a technologické. V následující sekcích jsou jednotlivé oblasti makrookolí popsány a je analyzován jejich současný stav.

Negativní výsledky analýzy pro Infosys znamenají možné omezení provozního rozpočtu a investic do IT infrastruktury, což sťažuje situaci implementace návrhů pro odstranění identifikovaných nedostatků v kapitole 5.2. Více teoretických poznatků a informací o analýze se nachází v kapitole 3.6.

### Politické a legislativní faktory

V současnosti je politická situace v České republice i ve světě poměrně volatilní. Nestabilní roztržštěná vláda neplní své sliby voličům spolu s odhalovanými korupčními skandály a vysokou inflací netvoří na domácím trhu přívětivé prostředí. Na druhou stranu hromadné propouštění ve výrobě a bankovním sektoru dává firmě možnost získat poměrně snadno nové pracovníky nově hledající práci na trhu, kde má převahu zaměstnavatel.

Protože většina vstupů do výroby je importována ze zahraničí a hotové produkty jsou také většinou exportovány do cizích zemí, je dalším vlivným faktorem kolísání kurzu koruny vůči euru a dolaru. Cena ropy, pohonných hmot a energií se sice za poslední rok stabilizovala, ale pořád zůstávají na vysoké úrovni a dále brzdí snižování inflace. Naopak

podpora elektromobility a zelené energie ze strany Evropské unie spolu s dalšími rozvojovými dotacemi pro průmysl přináší zajímavé příležitosti pro ty, kteří jsou dostatečně flexibilní a schopní se adaptovat podmínkám pro jejich získání.

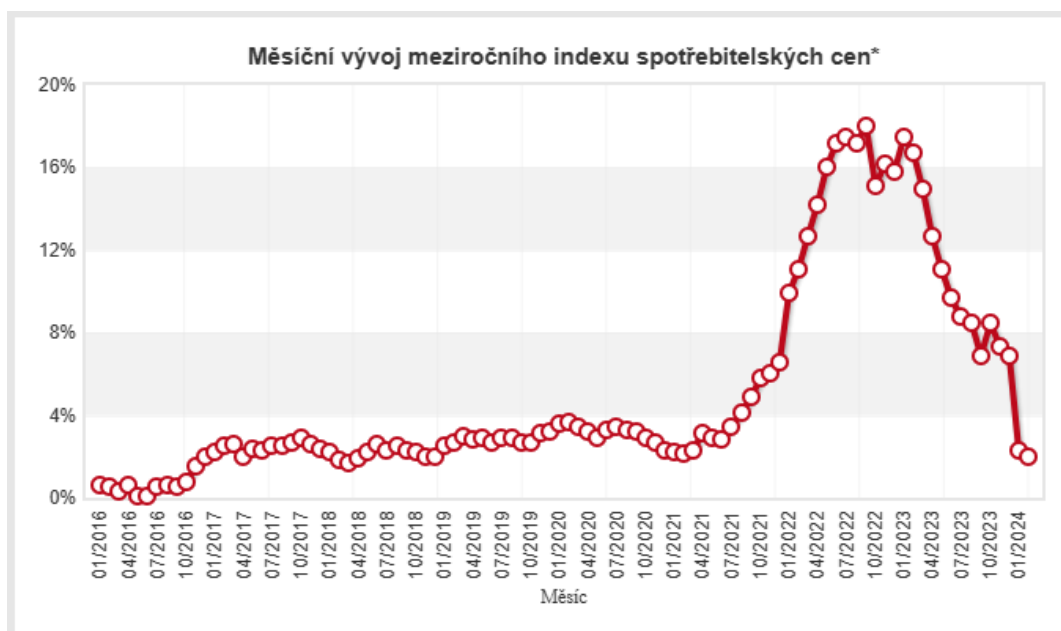
Geopolitické dění ve světě také nedodává jistotu – doznívající následky pandemie covid-19, trvající válka na Ukrajině, krvavý konflikt a hladomor v pásmu Gazy, radikální islámská hnutí na Blízkém východě, totální kolaps státu na Haiti, ruské hrozby jadernou válkou, Čína vyvíjející tlak na Tai-Wan a série ozbrojených státních převratů v oblasti Sahelu propukající v občanské války s podporou Francie je dlouhý list vážných problémů, se kterými se dnešní svět a lidé v zasažených oblastech potýkají.

## Ekonomické faktory

Do velmi silně působících ekonomických faktorů na společnost ABC se řadí výhody i nevýhody členství v Evropské unii, poslední dobou často zmiňovaná vysoká inflace, ceny energií a ceny pohonných hmot.

Evropská unie svými dotacemi přináší již výše zmíněné výhody a příležitosti, naopak ale svými nařízeními a zvýšenými požadavky na kvalitu produktů zvyšuje výrobní náklady, což je z druhého pohledu zajímavá příležitost pro výrobce v Asii a jiné státy mimo Evropskou unii.

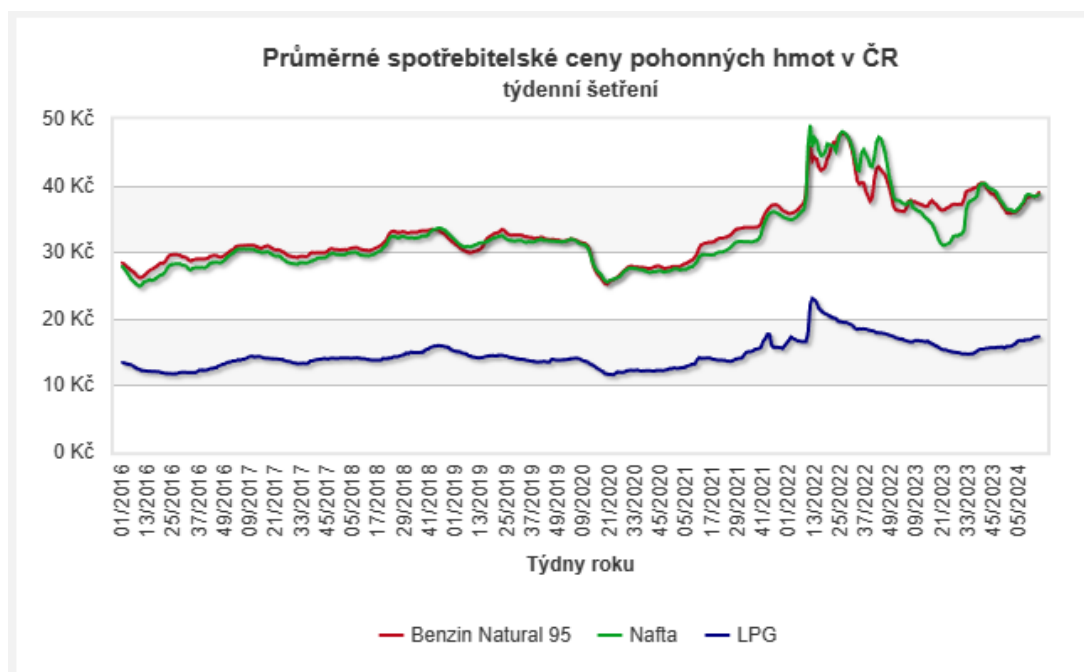
Vývoj inflace v posledních letech je poměrně děsivý jak pro běžné spotřebitele, tak pro podniky (viz graf 4.11). Inflace zvyšuje ceny vstupů a snižuje reálnou mzdu, což tvoří další riziko z pohledy spokojenosti zaměstnanců, jejichž zvyšování odměn nestíhá růst cen.



Obrázek 4.11: Vývoj inflace v České republice podle údajů Českého statistického úřadu. Zdroj: [7].

Dalším negativním faktorem je vysoká cena pohonných hmot (viz graf 4.12), které výrazně zvyšují ceny dopravy. Ty nejvíce ovlivňují firmy, které dováží a vyváží výrobky na dlouhé vzdálenosti, mezi které patří i ABC. Pohyby na trhu ropy jsou však celosvětový trend a zasahuje všechny podniky zhruba stejnou mírou, tudíž se nejedná o nevýhodu

pouze pro ABC.



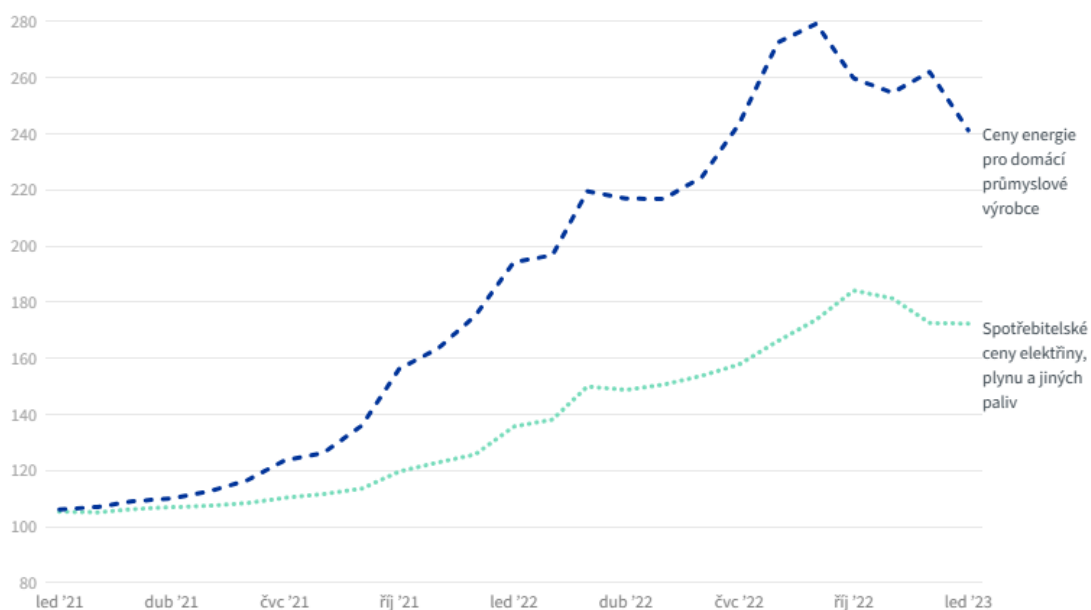
Obrázek 4.12: Vývoj cen pohonných hmot v České republice podle údajů Českého statistického úřadu. Zdroj: [8].

Posledním analyzovaným ekonomickým faktorem je cena energií v Evropské unii, která v roce 2022 dosáhla rekordní výše, viz 4.13. Ta se v souvislosti s ruskou invazí na Ukrajinu za poslední roky výrazně zvýšila, což má velký negativní dopad na všechny země EU a jejich obyvatele – obzvlášť pak v Česku po krachu Bohemia Energy a následnému chaosu na domácím trhu. Ceny energií nejen dále zvyšují výrobní náklady, zároveň i snižují vůli zákazníků investovat do výroby a strojů, které jejich spotřebu ještě více zvýší. Shrnutím analýzy ekonomických faktorů je, že současná makroekonomická situace není příznivá. Inflation sice v posledním roce klesá, výrobky si ale svoji cenovou hladinu vesměs drží po rapidním zdražování z předchozích let. Ceny pohonných hmot se opět ustálily, avšak na hladině, která je citelně vyšší oproti cenám před rokem 2022 a ceny energií, ač také pomalu klesají, netvoří svou výši příznivé ekonomické prostředí.

## Sociální faktory

Sociální faktory působí na ABC jako zdroj příležitostí, ale i jako zdroj hrozeb. V krátké dojezdové vzdálenosti od sídla firmy bydlí více než milion lidí, což poskytuje poměrně velký soubor potenciálních zaměstnanců a zjednodušuje situace, kdy je ABC nucena vyměnit nebo získat nové pracovníky. Další potenciál představuje ruská invaze na Ukrajinu a s ní spojená migrační vlna, která přináší ještě širší výběr zaměstnanců na trh práce.

Naopak negativně na ABC působí globální trend stárnutí a stagnace počtu obyvatel. Pro společnost to znamená úbytek zkušených specialistů s roky praxe a podnikatelé jsou často nuceni alespoň částečně najímat externí pracovníky – ti jsou ale dražší, je potřeba je důkladně proškolit v interních záležitostech a není jednoduché je sociálně integrovat do



Obrázek 4.13: Vývoj ceny energií v Evropské unii podle údajů Evropské rady. Na svislé ose je srovnání hodnoty s cenou v roce 2015, tzn. pokud graf zobrazuje hodnotu 200, je cena energie na 200 % oproti ceně v roce 2015. Zdroj: [4].

existujících týmů. Částečně proti následkům stárnutí populace však může působit v současnosti probírané zvýšení věku odchodu do důchodu. To sice nenabízí dlouhodobé řešení, avšak v několika dalších letech negativní sociální dopady zmírní. Další příležitost je tvořena samotnými zákazníky, kteří mají vzrůstající zájem o udržitelnost a ekologii. Pro společnosti to poskytuje prostor tvořit efektivní reklamní kampaně založené na udržitelnosti, společenské odpovědnosti a přitom udělat něco dobrého pro naši planetu a spoluobčany.

## Technologické faktory

Technologické faktory makroekonomického okolí na firmu ABC působí několika silnými trendy – tendencí neustálého zvyšování efektivity práce zaměstnanců, zvyšování kvality nabízených produktů a prodlužování jejich životnosti, přičemž by všechny tyto snahy měly zároveň snižovat negativní dopady na životní prostředí. Kombinace těchto vlivů zvyšuje náklady výroby a klade větší tlak na interní výzkum a zlepšování, čemuž se několik zaměstnanců společnosti ABC aktivně věnuje.

Naproti tomu dotace a podpora Evropské unie v oblasti elektromobility a získávání energie z obnovitelných zdrojů tvoří řadu příležitostí. Vznikají nové, stále efektivnější typy přístrojů pro tvorbu elektrické energie, technická úroveň elektromobilů a jejich součástí dlouhodobě roste se vznikem nových součástek a aplikací pokročilých technologií. Nově vznikající výrobní linky a postupy jsou obrovskou příležitostí pro výrobce měřicích přístrojů, mezi které patří i ABC. Právě ABC je schopno dodat na míru navržené a zkompletované stroje, které jsou schopny měřit s minimálními odchylkami nejen délky dílů, ale i další jejich vlastnosti, jakými jsou například hrubost povrchu nebo tvrdost.

Nová etapa automobilového průmyslu zaměřená na udržitelnost je zároveň velký trh, na kterém se ABC může prosadit.

## 4.5 Analýza metodou ZEFIS

Pomocí dotazníků interního auditu vyplněných zaměstnanci společnosti ABC byl schopen systém ZEFIS vypracovat seznam nalezených nedostatků spolu se zhodnocením jeho efektivity a bezpečnosti. Jednotlivé výstupy metody ZEFIS jsou popsány v následujících sekcích.

### Nedostatky informačního systému

Součástí této kapitoly je představení výstupu hodnotícího systému (viz obrázek 4.14) a vysvětlení jednotlivých nálezů. Analyzovaným procesem v dotazníku auditu procesu je proces zápisu docházky zaměstnanců včetně zaznamenání, jakým činností se v průběhu pracovní doby věnovali. Tuto činnost vykonává každý pracovník sám za sebe v modulu informačního systému Infosys.

Červeně vyznačené jsou vysoce významné nálezy, žluté jsou středně významné a zelené jsou méně důležité nedostatky.

| Oblast     | Významnost | Bezpečnost | Typ     | Název                                                           |
|------------|------------|------------|---------|-----------------------------------------------------------------|
| Pracovníci | Vysoká     | Ne         | Neshoda | Chybí zastupitelnost klíčových pracovníků pro informační systém |
| Pracovníci | Vysoká     | Ano        | Neshoda | Nastavení přístupových práv                                     |
| Zákazníci  | Vysoká     | Ano        | Neshoda | Nejsou nastavena pravidla práce s daty zákazníků                |
| Pracovníci | Vysoká     | Ano        | Neshoda | Nejsou aktualizovaná hesla uživatelů                            |
| Pravidla   | Střední    | Ano        | Neshoda | Chybějící, nebo špatně dodržovaná bezpečnostní pravidla         |
| Programy   | Střední    | Ano        | Neshoda | Pracovníci mohou instalovat programy na své počítače            |
| Pracovníci | Střední    | Ano        | Neshoda | Přístupová práva zaměstnanců nejsou správně ukončována          |
| Pracovníci | Střední    | Ne         | Neshoda | Níže kvalifikace a schopnosti pracovníků v procesu              |
| Pravidla   | Střední    | Ne         | Neshoda | Špatně stanovená zodpovědnost pracovníků v procesu              |
| Zákazníci  | Střední    | Ne         | Neshoda | Chybí průzkumy spokojenosti zákazníků                           |
| Pravidla   | Střední    | Ano        | Neshoda | Nejsou pravidla a postupy, jak se provádí proces                |
| Programy   | Střední    | Ne         | Neshoda | Pracovníkům chybí některá data nebo funkce                      |
| Pracovníci | Střední    | Ano        | Neshoda | Bezpečnostní hrozba z přístupu na internet                      |
| Data       | Střední    | Ano        | Neshoda | Riziko zneužití dat, virového útoku                             |
| Technika   | Nízká      | Ne         | Neshoda | Riziko zbytečných nákladů z nekompatibilní techniky             |
| Programy   | Nízká      | Ne         | Neshoda | Chybějící nebo špatně dostupné návody pro práci se systémem     |
| Technika   | Nízká      | Ano        | Neshoda | Špatné fyzické zabezpečení klíčových prvků infrastruktury       |
| Data       | Nízká      | Ano        | Neshoda | Odpovědnost pracovníků za data                                  |
| Provoz     | Nízká      | Ne         | Neshoda | Není známo, jak jsou příjemci spokojeni s výstupy procesu       |

Obrázek 4.14: Výstup systému ZEFIS obsahující analýzu nedostatků. Červeně označeny jsou závažné chyby, žlutě označeny jsou chyby se středním dopadem a zeleně vyznačené jsou méně důležité nedostatky. Zdroj: [16].

## Nedostatky v oblasti dat

Následující podsekce se věnuje nedostatkům odhaleným systémem ZEFIS v oblasti dat. Stručně představí jejich podstatu a popíše možné dopady.

- **Riziko zneužití dat, virového útoku**

Hrozby kybernetických útoků jsou velmi často opomíjeny, poněvadž investice do jejich snížení bývají poměrně vysoké a nepřinášejí přidanou hodnotu. Většina společností tedy začne brát ochranu před virovými napadeními až po útoku, kdy už je pozdě a škody byly napáchány. Hrozí totiž narušení dostupnosti, integrity dat či jejich důvěrnosti. Hrozí také zašifrování dat na discích a vymáhání výpalného za jejich dešifrování, ke kterému ani nemusí dojít (tzv. *ransomware*), případně jejich zcizení a zneužití vedoucí k žalobám od zákazníků. V dnešní době čím dál častěji skloňovaných válek v kyberprostoru se jedná o riziko, které by nemělo být podceňováno.

- **Odpovědnost pracovníků za data**

Pracovníci nemají jednoznačně určeno, kdo zodpovídá za která data. Je tedy nutno přesně tyto odpovědnosti určit, definovat kdy by taková data měla být zaváděna do systému a jejich postupy pravidelně kontrolovat. V opačném případě hrozí narušení integrity (viz 3.5) a kvality dat do bodu, kdy báze dat již nemusí odpovídat skutečnosti. Na chybných datech pak pochopitelně nelze zpracovat důvěryhodné analýzy a stavět na nich informovaná rozhodnutí.

## Nedostatky v oblasti pracovníků

Následující podsekce se věnuje nedostatkům odhaleným systémem ZEFIS v oblasti pracovníků. Stručně představí jejich podstatu a popíše možné dopady.

- **Chybí zastupitelnost klíčových pracovníků pro informační systém**

V každé společnosti jsou pracovníci, kteří jsou z nějaké perspektivy klíčoví – ať už se jedná o jejich znalosti interních záležitostí, odbornou expertizu v odvětví nebo kontakty s vnějším prostředím firmy. Management by měl takové zaměstnance identifikovat a zajistit, že v případě kdy klíčový pracovník dlouhodobě onemocní či odejde ze zaměstnání, nebude se jednat o vážnou ránu pro fungování společnosti. Snaha managementu by měla směřovat k přípravě alespoň jednoho dalšího zaměstnance pro takovou situaci a zajistit předávání potřebných znalostí z klíčového pracovníka na jiné kolegy.

- **Nastavení přístupových práv**

Pro každou společnost je důležité mít funkční a aktuální systém přidělující oprávnění jednotlivým uživatelům. Zaměstnanci sice o práva žádají, ale při přesunu do jiné funkce nebo úplného odchodu z firmy se již nehlásí o jejich odebrání. Zanedbání správného odebrání přístupových práv je závažná bezpečnostní hrozba a je nutné mít systém spravující tato oprávnění správně nastaven a aktuální.

- **Nejsou aktualizovaná hesla uživatelů**

Mít správně nastavenou politiku hesel výrazně zvyšuje bezpečnost systému jako celku. Pokud je zaměstnancům dovoleno používat jakákoliv hesla, řada z nich si

vybere heslo které je příliš jednoduché a prolomitelné. Za silné heslo je považováno takové, které obsahuje alespoň osm znaků s kombinací malých písmen, velkých písmen, číslic a speciálních znaků. Správci bezpečnost hesel se také často uchylují k povinné změně hesel za určité období, avšak zde je otázkou, zda to nevede naopak ke snížení bezpečnosti – zaměstnanci pak svá hesla často zapisují na lístky nebo do sešitů, které zanechávají volně na svém pracovním stole, kam se k nim může dostat prakticky kdokoli.

- **Přístupová práva zaměstnanců nejsou správně ukončována**

Nedostatek ukončování práv úzce souvisí s nedostatkem *Nastavení přístupových práv* jenž byl popsán výše. Při odchodu zaměstnance je opravdu potřeba se ujistit, že mu jsou správně odebrány práva. Po rozhodnutí o přesunutí daného zaměstnance nebo ukončení pracovního poměru by tato zpáva měla okamžitě být předána správci zodpovědnému za management přístupových oprávnění – je tedy nutná spolupráce mezi personalisty a oddělení IT.

- **Nižší kvalifikace a schopnosti pracovníků v procesu**

Nedostatečná kvalifikace zaměstnanců má pochopitelně nezanedbatelný vliv na efektivitu a společnost jako takovou. Je v zájmu firmy své zaměstnance školit a vzdělávat, čímž budou při své činnosti výkonnější a budou dělat méně chyb.

- **Bezpečnostní hrozba z přístupu na internet**

Přístup na internet je povětšinou pro znalostní pracovníky nutnost, avšak přichází s ním také řada rizik spojených s virovými útoky a phishingem. Pokud se ve společnosti nachází zaměstnanec pracující s citlivými firemními daty a zároveň nutně nepotřebuje přístup k internetu, je vhodné toto riziko eliminovat úplně. Avšak je třeba brát na vědomí, že zaměstnanci takové opatření neuvítají a mělo by být aplikováno jen ve vážně odůvodněných případech.

## **Nedostatky v oblasti pravidel**

Následující podsekcce se věnuje nedostatkům odhaleným systémem ZEFIS v oblasti pravidel. Stručně představí jejich podstatu a popíše možné dopady.

- **Chybějící, nebo špatně dodržovaná bezpečnostní pravidla**

V případě, kdy jsou špatně nastavena ve společnosti bezpečnostní pravidla vzniká několik hrozeb. Systémy jsou náchylnější k útokům, například pokud zaměstnanci nepoužívají silná hesla nebo neaktualizují nainstalovaný software, stávají se snadnějšími cíli pro útočníky. Podobně v případě kdy je špatně zavedena správa oprávnění, hrozí riziko neoprávněného přístupu osob, jenž může vést k ohrožení důvěrnosti, integrity a dostupnosti (viz 3.5). Je důležité, aby organizace dbaly na dodržování bezpečnostních postupů a pravidelně prováděly audit a školení zaměstnanců, aby minimalizovaly riziko spojené s nedodržováním těchto pravidel.

- **Špatně stanovená zodpovědnost pracovníků v procesu**

Obecně platí, že za každou činnost musí být zodpovědný právě jeden zaměstnanec nebo konkrétní role přidělována zaměstnancům a musí si toho být všichni vědomi. Pokud tomu tak není, pak dříve nebo později nastane situace, kdy se každá

odpovědná osoba domnívá, že daný úkol řeší někdo jiný. Ve výsledku vznikají zmatky, nedorozumění a značné zpoždění, která mohou mít velmi vážné následky – od nedodržení termínů, přes spory v týmech a úpad morálky až po odchod přepracovaného zaměstnance, který po celou dobu danou zodpovědnost vykonával sám bez cizí pomoci.

### **Nedostatky v oblasti zákazníků**

Následující podsekce se věnuje nedostatkům odhaleným systémem ZEFIS v oblasti zákazníků. Stručně představí jejich podstatu a popíše možné dopady.

- **Nejsou stanovena pravidla práce s daty zákazníků**

Ochrana citlivých dat zákazníků je velmi důležitou povinností každé společnosti, která je zakotvena i na mezinárodní úrovni v podobě GDPR[41] (z anglického General Data Protection Regulation). Pokud s daty společnost zachází nezodpovědně a nevěnuje dostatečné úsilí jejich bezpečnému uchovávání, může to vést k vysokým pokutám, ztrátě reputace a důvěry klientů. Je tedy nutné pevně stanovit a vynucovat pravidla, kteří zaměstnanci mohou různými způsoby manipulovat se zákaznickými daty a to vše ve shodě s legislativou.

- **Chybí průzkumy spokojenosti zákazníků**

Získat nové zákazníky je znatelně nákladnější, nežli si udržet ty stávající – proto je důležité mít přehled jak o jejich spokojenosti s nabízenými produkty, ale i počty reklamací a stížností. Průzkumy spokojenosti také poskytují cennou zpětnou vazbu a pomáhají identifikovat slabé místa *customer relationship managementu*.

### **Nedostatky v oblasti programů**

Následující podsekce se věnuje nedostatkům odhaleným systémem ZEFIS v oblasti programů. Stručně představí jejich podstatu a popíše možné dopady.

- **Pracovníci mohou instalovat programy na své počítače**

Pokud společnost nechává zaměstnancům volnou ruku při správě softwaru na svých počítačích, pak jsou sice pracovníci flexibilnější a mohou pracovat se svými oblíbenými programy podle libosti, avšak přináší to rizika. Prvním rizikem je virový útok, který vědomě či nevědomě uživatel umožní stažením infikovaného softwaru. Druhým rizikem je dodržování licenčních pravidel – zaměstnanec totiž může stáhnout nelegální kopii licencovaného programu, nebo při výběru licence uvést sebe například jako studenta. V takovém případě používá zdarma program, který je pro komerční užití placený a odpovědnost nese zaměstnavatel. Třetím rizikem je skutečnost, že pokud různí pracovníci používají ten samý program, nemusí již používat tu samou verzi a sdílení jejich výsledků může působit potíže a zbytečné náklady navíc.

- **Pracovníkům chybí některá data nebo funkce**

V případě kdy informační systém neposkytuje všechnu potřebnou funkcionalitu nebo informace pro své uživatele, vzniká práce navíc. Uživatel musí chybějící informace najít sám nebo s pomocí svých kolegů a chybějící funkcionalitu musí často dělat ručně, což mnohdy velmi výrazně snižuje efektivitu práce.

- **Chybějící nebo špatně dostupné návody pro práci se systémem**

Pokud pro systém neexistuje dostatečně podrobná, nebo naopak příliš podrobná a nepřehledná dokumentace s návody pro práci s informačním systémem, je pro zaměstnance obtížné s ním bez patřičného školení pracovat. Zvyšuje se jejich chybovost a pro každou chybu je čas nápravy prodloužen, protože nemají dostatek podkladů a znalostí zjednat nápravu v rychlejším čase.

## **Nedostatky v oblasti techniky**

Následující podsekcce se věnuje nedostatkům odhaleným systémem ZEFIS v oblasti techniky. Stručně představí jejich podstatu a popíše možné dopady.

- **Riziko zbytečných nákladů z nekompatibilní techniky**

Při nákupu technických prvků je potřeba se ujistit, že tato technika bude funkční a schopna pracovat s již existující technikou společnosti. Pokud technika nebude schopna spolupracovat, hrozí problémy například s kompatibilitou softwarových verzí vyžadující nastavení a migraci na jiný systém nebo hrozí duplikace funkcionality a jejich roztržnění, což výrazně snižuje přehlednost, zvyšuje pracnost a zvyšuje počet potřebných licencí. Neověřování si takových skutečností dopředu může vést ke spoustě zbytečné práce a nákladů, které v nejhorším případě vedou až ke ztrátě konkurenčních výhod.

- **Špatné fyzické zabezpečení klíčových prvků infrastruktury**

Ve firmě ABC se servery a další klíčové prvky fyzicky nachází v prostorách kanceláře, čímž vzniká nutnost je náležitě chránit. Vážou se k nim totiž hrozby, jakými jsou například zcizení prvků či dat, jejich vandalismus a živelné katastrofy. Ochrana před neoprávněným přístupem je v tomto případě klíčová a měla by jí být věnována velká pozornost, spolu s duplikací dat na fyzicky odděleném místě.

## **Nedostatek v oblasti provozu**

Následující podsekcce se věnuje nedostatku odhaleným systémem ZEFIS v oblasti provozu. Stručně představí jeho podstatu a popíše možné dopady.

- **Není známo, jak jsou příjemci spokojeni s výstupy procesu**

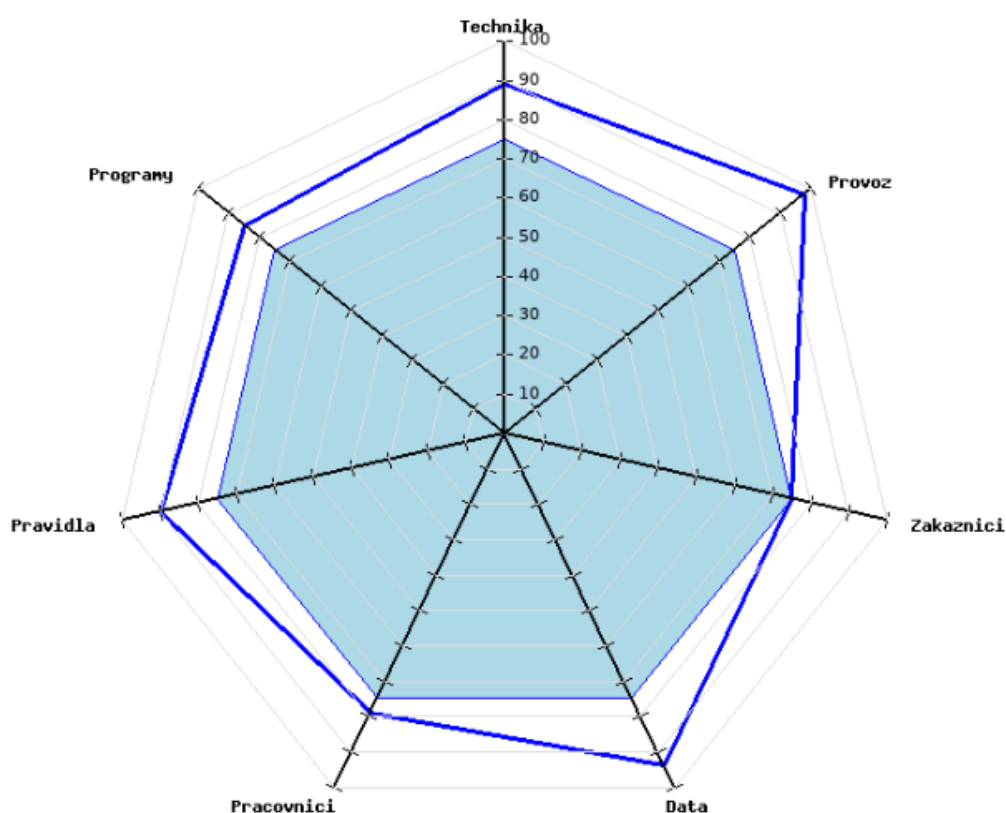
Jelikož jsou procesy ve firmě provázány a výstup jednoho může sloužit jako vstup druhého, je vhodné vědět od pracovníků využívající výstup zda a do jaké míry s ním jsou spokojeni. V případě auditu procesu zadávání docházky a času stráveného jednotlivými úkoly je výstupem seznam všech pracovníků, kteří došli daný den do práce a čemu se věnovali. Zaměstnanci využívající seznam jako svůj vstup jsou primárně ti zodpovědní za lidské zdroje a administrativa účtující zákazníkům faktury za provedenou práci. Ve firmě ABC se jejich spokojenost s výstupem neřeší a v případě kdy jsou silně nespokojeni, hrozí nekvalitní odvádění práce a snížení jejich morálky.

## **Efektivita informačního systému**

V kontextu analýzy provedené metodou ZEFIS značí pojem efektivnost informačního systému stupeň dosažení stanoveného cíle. Cílem v našem případě jsou správně vybrané,

nastavené a provozované informační systémy a procesy firmy, bez nedostatků a chyb. Společnost by se měla snažit vyváženého řešení bez výrazně slabších nebo silnějších článků, poněvadž z pohledu metody ZEFIS je pak takový systém nejvíce efektivní s nejnižšími náklady.

Je vhodné dodat, že efektivnost je zde počítána jako procento ze součtu nedostatků vynásobených jejich váhou oproti dvojnásobku součtu hodnot shod a nedostatků v rámci daného typu zkoumané firmy. Výsledná hodnota se pohybuje v rozmezí mezi 50 % a 100 %. Výsledek 50 % značí porušení všech doporučovaných postupů, naopak 100 % platí pro plný soulad s ideálním stavem pro danou firmu[16].



Obrázek 4.15: Výsledek efektivnosti informačního systému. Hodnoty na osách jsou udávány v procentech, fialová čára značí efektivitu v jednotlivých oblastech a modře vyplněná oblast značí celkovou úroveň efektivity informačního systému. Zdroj: [16].

Obrázek 4.15 znázorňuje výsledky spočtené portálem ZEFIS. Zjištěná celková efektivita informačního systému je 75 %, což není ani špatný, ani dobrý výsledek. V oblasti zákazníků a pracovníků Infosys nijak neexceluje, zato v oblastech dat a provozu si vede velice dobře. Pokud má společnost ABC zájem zvýšit efektivitu svého informačního systému, měla by se věnovat zejména oblasti zákazníků a pracovníků. Přesné hodnoty v jednotlivých oblastech jsou znázorněny v obrázku 4.16.

| Oblast        | Moje firma |
|---------------|------------|
| Technika      | 89%        |
| Programy      | 85%        |
| Pravidla      | 90%        |
| Pracovníci    | 79%        |
| Data          | 94%        |
| Zákazníci     | 75%        |
| Provoz        | 98%        |
| <b>Celkem</b> | <b>75%</b> |

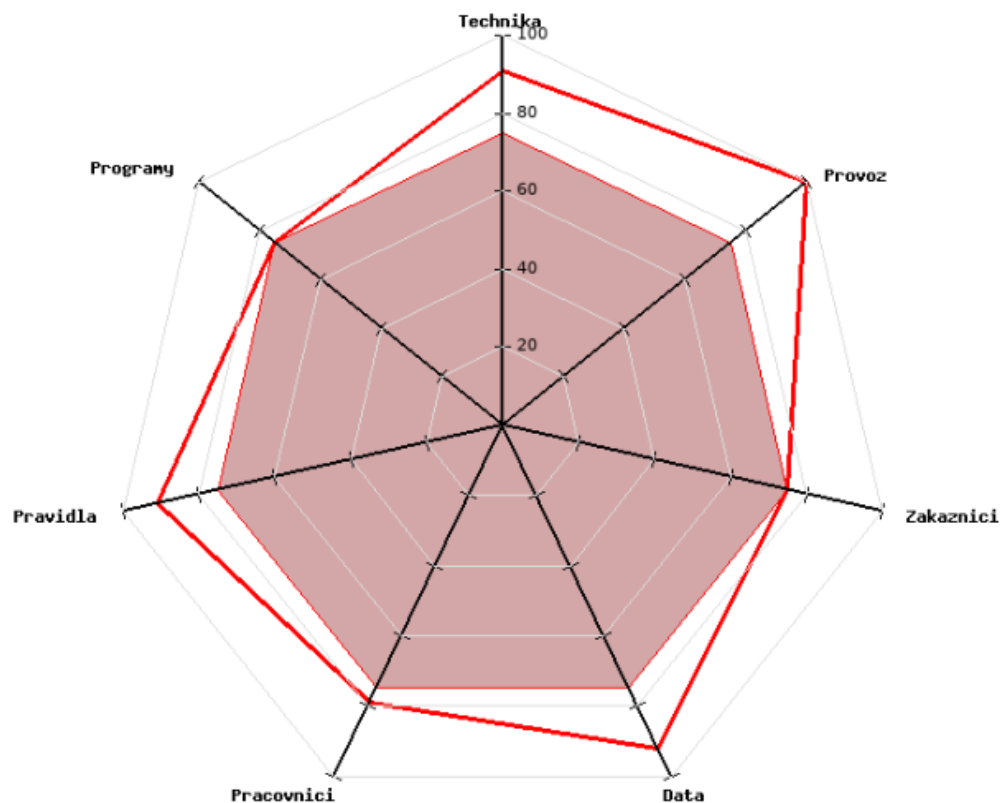
Obrázek 4.16: Detailní výsledky efektivity metody ZEFIS. Zdroj: [16].

## Bezpečnost informačního systému

V hodnocení bezpečnosti nebere portál ZEFIS v potaz pouze zkoumaný Infosys, nýbrž zahrnuje do své analýzy i firmu jako takovou spolu se všemi procesy. Zobrazuje úroveň bezpečnosti podle nalezených nedostatků v jednotlivých oblastech a stejně jako u efektivnosti platí, že celková bezpečnost je dána nejslabším článkem.

Samotný výpočet hodnoty bezpečnosti probíhá tak, že výsledné hodnotě přiřadí procento ze součtu nedostatků v oblasti bezpečnosti násobených jejich váhou oproti dvojnásobnému součtu hodnot shod a nedostatků v oblasti bezpečnosti, relevantních pro daný typ firmy. Výsledek se tedy nachází v rozmezí mezi 50 a 100 procenty, přičemž 50 % znamená, že všechny testované bezpečnostní zásady byly porušeny a 100 % znamená plnou shodu s ideálním stavem daného typu firmy[16].

Obrázek 4.17 znázorňuje výsledky spočtené portálem ZEFIS. Zjištěná celková bezpečnost je 75 %, tedy vcelku průměrný. V oblasti zákazníků, programů a pracovníků Infosys nijak neexceluje, zato v ostatních oblastech techniky, pravidel, dat a provozu dosáhl velmi dobrých výsledků, přičemž oblast provozu byla ohodnocena 100 %. Pokud má společnost ABC zájem zvýšit svoji bezpečnost, měla by se věnovat zejména oblasti zákazníků, programů a pracovníků. Přesné hodnoty v jednotlivých oblastech jsou znázorněny v obrázku 4.18.



Obrázek 4.17: Výsledek bezpečnosti informačního systému. Hodnoty na osách jsou udávány v procentech, světle červená čára značí bezpečnost v jednotlivých oblastech a tmavě červeně vyplněná oblast značí celkovou úroveň bezpečnosti informačního systému. Zdroj: [16].

| Oblast     | Moje firma |
|------------|------------|
| Technika   | 91%        |
| Programy   | 75%        |
| Pravidla   | 91%        |
| Pracovníci | 79%        |
| Data       | 92%        |
| Zákazníci  | 75%        |
| Provoz     | 100%       |
| Celkem     | 75%        |

Obrázek 4.18: Tabulka s detailními výsledky bezpečnosti metody ZEFIS. Zdroj: [16].

## Kapitola 5

# Identifikace nedostatků a návrhy vylepšení informačního systému

Následující stěžejní kapitola diplomové práce staví na teoretických poznatcích z kapitoly 3, pomocí kterých byl v kapitole 4 rozebrán současný stav nejen samotné společnosti ABC, ale i jejího informačního systému pomocí metody ZEFIS a vnějšího makrookolí analýzou Porterova modelu pěti sil a analýzy PEST.

Nově získané poznatky jsou v této kapitole využity k odhalení relevantních nedostatků a návrhů akcí, jenž může ABC podniknout pro snížení jejich dopadu nebo úplnou eliminaci hrozeb. V kapitole 6 je pak rozvedeno ekonomické vyhodnocení jejich přínosů a nákladů.

### 5.1 Identifikace a rozbor nalezených nedostatků

První ze dvou sekcí této kapitoly vyjmenovává odhalené chyby, popisuje jejich podstatu a zabývá se hrozbami, které pro společnost ABC vytváří. Způsoby jak hrozby mitigovat nebo jim úplně předejít pak představuje druhá sekce stejné kapitoly, viz 5.2. Každá z následujících podsekcí se věnuje jednomu z identifikovaných nedostatků.

#### 5.1.1 Zaměstnancům je umožněno manipulovat s cizími soubory

Skutečnost, že zaměstnanci mohou jeden druhému modifikovat či úplně odstranit dokumenty nebo výkresy je obrovskou hrozbou. V minulosti již nastal případ, kdy zaměstnanec ABC zneužil této bezpečnostní slabiny, přečetl si vysoce citlivé informace o zakázce a ty poté zneužil. Od té doby je sice přístup k modulu Zakázek omezen pomocí zvláštního oprávnění, avšak riziko zůstává pro ostatní dokumenty, moduly a řadu informací obsažených v Infosysu. Jedná se o velmi snadný způsob, jak mohou zaměstnanci úmyslně či neúmyslně vážně poškodit dokumentaci firmy, pracovní morálku nebo reputaci mezi klienty.

Hrozba by neměla být podceňována a co nejdříve zavedena potřebná protipatření jenž přinejmenším sníží riziko na přijatelnou úroveň, viz podsekcce 5.2.6 – v opačném případě může společnost brzy čelit vysokým škodám a vážným právním následkům.

#### 5.1.2 Rizika spojená s ochranou osobních údajů zaměstnanců

Legislativa Evropské unie General Data Protection Regulation, více známá pod zkratkou GDPR[41], funguje jako ochrana soukromí osob garantovaná na mezinárodní úrovni.

Podniky jsou nuceny dodržovat řadu pravidel ohledně uchovávání, mazání a sdílení osobních informací, které často není jednoduché implementovat. Navíc ne vždy se zákon vyjadřuje jasně a může být zapotřebí i konzultace s právníkem.

Společnost ABC se GDPR řídí, avšak pouze vůči zákazníkům a externím společnostem. Problém vyvstává při manipulaci s daty zaměstnanců, kde společnost ABC nevyvalovala mnoho úsilí legislativní pravidla dodržet a pro jediného tvůrce systému Infosys to není vůbec lehký úkol. Infosys je vyvíjen již roky bez aplikování nejlepších praktik pro vývoj softwaru a v tomto bodě je již velmi obtížné do programu výrazně zasahovat. Implementace funkcionality takovým způsobem, aby byla v souladu s nařízením GDPR by pak vyžadovala spoustu času a velké úsilí autora Infosysu spolu s dalšími náklady spojenými s právním rozbořením, zda nová verze evropské podmínky splňuje. Další práce by čekala i správce IT infrastruktury společnosti ABC, protože by připadlo jim zařídit uchovávání dat takovým způsobem, aby byl v souladu s právem.

Návrhu jak zlepšit současný stav se podrobněji věnuje a rozvádí sekce 5.2.1.

### 5.1.3 Chybí šifrování úložiště

Zanedbání ochrany dat na fyzických úložištích představuje významnou bezpečnostní hrozbu. Nezašifrovaná data mohou být snadno kompromitována v případě kdy dojde k neoprávněnému přístupu, ať už interně nebo externí entitou. Bez šifrování jsou data přístupná každému, kdo má fyzický přístup k těmto úložištím – včetně zaměstnanců, kteří nejsou oprávněni s informacemi obsaženými na paměťových médiích manipulovat.

Kromě toho absence šifrování dat představuje hrozbu v případě, kdy dojde ke ztrátě nebo odcizení hardwarových prvků s uloženými daty. Pokud se úložiště dostanou k útočníkovi, mohou obsažené informace, včetně citlivých údajů zákazníků, obchodních tajemství nebo interních dokumentů, být zneužity ku prospěchu konkurence, útočníka nebo jako účinná zbraň poškozující společnost ABC. To může vést k právním následkům, ztrátě důvěryhodnosti společnosti a vážnému poškození jejího obchodního postavení.

Návrh jak zlepšit stav Infosysu v ohledu šifrování dat přibližuje podsekce 5.2.3.

### 5.1.4 Ruční nastavování jednotlivých práv každému uživateli

V situaci jako ve společnosti ABC, kdy jeden správce systému manuálně přiděluje a odebírá přístupová oprávnění jednotlivě každému uživateli zvláště pro každou složku, existuje významné bezpečnostní riziko spojené s nedostatečnou kontrolou přístupu k datům. Postup ručního přidělování je náchylný k chybám, opomenutím a nedbalosti, což může vést k přidělení práva osobě, která jej nepotřebuje (porušení principu *need to know*) nebo naopak neodstranění pravomoci zaměstnanci, jehož pracovní poměr byl ukončen nebo byl přesunut na jinou pracovní pozici.

Dále tato manuální správa přístupových práv neumožňuje efektivní sledování a auditování přístupů k datům. Bez centrálního systému managementu oprávnění není možné snadno identifikovat, kdo má přístup k jakým záznamům a jakým způsobem s nimi manipuluje. Tento nedostatek transparentnosti tvoří podmínky pro neetické chování a akci v nesouladu s bezpečnostními předpisy, jakými jsou například zneužití dat, krádež obchodního tajemství nebo porušení zásad ochrany osobních údajů.

Možný způsob jak předejít souvisejícím problémům a snížit chybovost v procesu přidělování práv představuje sekce 5.2.2.

### 5.1.5 Nedostatečně časté zálohování dat z MS Access souborů

Zálohování dat je klíčovou součástí mitigace hrozek spojených s uchováváním informací. V podsekcí 4.2.2 diplomové práce jsou uvedeny podrobnosti procesu zálohování dat ve firmě ABC, avšak tato podsekcce se věnuje pouze jeho menší části – zálohování dat v aplikaci MS Access. Textová data obsažená v souborech aplikace jsou velmi citlivé povahy, ať už se jedná o osobní informace zaměstnanců, jejich platy, údaje o zakázkách nebo kontaktní informace klientů společnosti ABC.

Ztráta všech takových údajů najednou může v okamžiku zničit léta budovanou firmu a proto se ABC drží správné myšlenky informace zálohovat. Činit tak jedenkrát ročně u natolik kritických dat však není dostačující – během jednoho roku může podnik nabrat řadu nových zakázek, získat cenné kontakty a vytvořit spoustu výkresové dokumentace, jejichž ztráta by způsobila velký chaos. Současný stav je tedy z pohledu zálohování textových dat MS Access silně nedostačující a způsobům jak jej vylepšit se věnuje podsekcce 5.2.5.

### 5.1.6 Nezastupitelnost externího tvůrce systému

Vývoj Infosysu začal interně ještě před rokem 2000 a během jeho celého životního cyklu na něm pracoval jediný člověk, v té době zaměstnanec ABC. Tvůrce systému sám soustřeďuje u sebe úplně všechny znalosti a zkušenosti, které použil nebo získal za tu dobu, čímž se stal pro firmu naprosto nenahraditelným. Jeho silnou pozici ještě dále upevnil tím, že dokumentaci kódu buďto netvořil vůbec, nebo ji s nikým nesdílel. Ve výsledku se tím stal pro společnost ABC klíčovou osobou a nadále jí zůstává i léta po ukončení jeho pracovního poměru.

V současnosti nikdo jiný není Infosysu jakkoliv modifikovat a pokud se požadavky ABC výrazně změní, je možné že ani původní tvůrce systému nebude ochoten funkcionalitu implementovat. V takovém případě pak nezbyvá podniku ABC jiná možnost, než provoz celého systému ukončit a plně přejít na nový. Navíc kvůli tomu, že tvůrce nepočítal s možností migrace dat na nový systém, jsou informace uloženy poněkud nestandardně. Jejich přenos není technicky jednoduchý úkol, což dále komplikuje situaci jenž s největší pravděpodobností jednoho dne nastane.

Naprostá nezastupitelnost autora Infosysu, který se navíc blíží důchodovému věku, tak představuje velkou slabinu společnosti ABC v systému, který pro ni obstarává ty nejdůležitější úkony a procesy.

### 5.1.7 Překlepy a chyby v textu uživatelského rozhraní

Uživatelské rozhraní Infosysu je dostupné pouze v českém jazyce, avšak i přesto se do něj promítnou jazykové nekonzistence, například modul pojmenován PERSONS. Název modulu zároveň poukazuje na další druh nekonzistencí, kterým je nepatřičné použití hůlkového písma v kontextu, kdy podobné názvy jsou psány běžným způsobem. V Infosysu se také vyskytují překlepy nebo zkratky použité neintuitivně, což dále snižuje uživatelův komfort. Ač se v systému nedostatky vyskytují, nečiní to z Infosysu nepoužitelný software. Překlepy, anglické termíny nebo hůlkové písmo působí spíše úsměvně než jako překážka v práci a neintuitivní použití zkratk také netvoří vysoké bariéry v uživatelském chápání funkcionality systému. Vylepšení uživatelského rozhraní spolu s dalšími návrhy zlepšení uvádí sekce 5.2.4.

## 5.2 Návrhy na zlepšení současného stavu

V této sekci se nachází podrobné popisy možných vylepšení odhalených nedostatků současného řešení, jejichž analýza se nachází v předchozí sekci 5.1. Pro nalezené nedostatky jsou zde odpovídající sekce s konkrétními změnami, které může ABC implementovat a tak celkově zlepšit svůj informační systém.

Vyhodnocení očekávaných přínosů a dopadů implementace změn pak popisuje následující kapitola 6, ve které lze najít i finanční odhad nákladů.

### 5.2.1 Úprava firemních procesů v souladu s GDPR

Proces změny managementu dat zaměstnanců takovým způsobem, aby dodržoval unijní předpis GDPR[41] je poměrně dlouhý projekt, který se dotkne fungování společnosti nejen z technické, ale i byznysové strany. Na jednu stranu nepřinese vesměs žádnou přidanou hodnotu pro firmu, na stranu druhou, pokud na společnost ABC zamíří žaloba kvůli porušování zákonů, znamená to problémy pro celou společnost – viz podsektory o nedostatku 5.1.2.

Vyšším managementem řízená změna by se v praxi měla věnovat primárně následujícím bodům:

- **Audit a klasifikace dat**

Prvím krokem je důkladné prošetření, se kterými daty společnost ABC manipuluje a identifikace těch, která spadají do rozsahu GDPR. Ty je pak potřeba klasifikovat přinejmenším na veřejně dostupná, interní a citlivá podle stupně jejich ochrany a podle toho s nimi i nakládat.

- **Zajištění náležitosti právního základu**

Podle GDPR je potřeba mít právně zakotvený souhlas zaměstnanců o zpracování jeho údajů. Tím může být například přidělený souhlas, součást smlouvy s protistranou nebo oprávněný zájem společnosti ABC. V případě kdy je souhlas poskytován protistranou, je důležité, aby byl formulován jasně a poskytován dobrovolně.

- **Uchovávání jen těch nejnutnějších dat**

Je doporučeno sbírat pouze ty informace, které jsou nezbytně nutné pro firmu – pokud společnost sbírá zbytečné informace, hrozí jí, že v jejich managementu udělá chybu a pravidla GDPR poruší.

- **Zavedení bezpečnostních opatření**

Při nakládání s daty je třeba mít na paměti jejich bezpečnost a nastavit technickou infrastrukturu a procesy takovým způsobem, aby pomáhaly bezpečnost udržovat. Dobrými kroky jsou zavedení šifrování (viz podsektory 5.2.3), správná správa přístupových práv (viz podsektory 5.2.2), interní bezpečnostní audity a udržování pravidel v povědomí zaměstnanců pomocí školení nebo infografik viditelných v prostorách firmy.

- **Umožnění subjektům využít jejich práva**

GDPR přisuzuje subjektům práva na přístup ke svým datům, jejich opravu, výmaz nebo v jiných případech mohou také žádat o omezení jejich zpracovávání. Je ale důležité zaměstnancům v rámci zákona takové kroky umožnit.

- **Udržování krizového plánu pro případ úniku dat**

Je důležitá příprava pro případy kdy dojde k porušení bezpečnosti dat. Společnost by měla vypracovat plán jak detekovat, hlásit a reagovat v takové situaci, včetně upozornění dozorčích orgánů a dotčených subjektů. Správně vypracovaný krizový plán pak pomůže ABC minimalizovat vzniklé škody a snížit negativní dopady na jejich reputaci a důvěru.

- **Pravidelné audity dodržování stanovených postupů**

Jakmile jsou provedené změny uvedeny do provozu, je nutné se k nim pravidelně vracet a aktualizovat je. Neméně důležité je se ujišťovat, že i zaměstnanci je berou vážně a pracují v souladu s předpisy GDPR.

Realizací uvedených bodů společnost zlepší své procesy a zajistí soulad s požadavky GDPR, čímž ochrání práva na ochranu soukromí svých zaměstnanců. Změny jsou rozsáhlé a netýkají se pouze Infosysu, avšak rozhodne-li se management je implementovat, vyhne se vysokým pokutám a devastujícím dopadům ztráty důvěry klientů.

### 5.2.2 Zavedení uživatelských skupin

V současnosti je jeden člověk zodpovědný za manuální přidělování systémových oprávnění, což tvoří prostor pro chyby obzvláště v případě, kdy odejde zaměstnanec ze společnosti (více o souvisejících hrozbách viz 5.1.4).

K minimalizaci tohoto bezpečnostního rizika je vhodným řešením implementovat centrální systém správy přístupových práv, jenž umožní zjednodušené přidělování a odebrání oprávnění na základě rolí a odpovědností zaměstnanců společnosti ABC. Takový systém by měl být také schopen poskytovat podrobné záznamy o uživatelských aktivitách, aby bylo možné účinně sledovat přístup k datům a identifikovat potenciální bezpečnostní incidenty.

Řešením splňujících stanovené požadavky je implementace RBAC (zkratka anglického *role-based access control*). RBAC systém neopravňuje jednotlivé uživatele zvláště, nýbrž oprávnění uděluje uživatelským skupinám, do kterých pak jednotlivé uživatele přidává.

Management společnosti ABC může RBAC implementovat následujícím způsobem:

1. **Rozbor aktuálních přístupových požadavků**

Prvním krokem je zhodnocení aktuální struktury oprávnění a identifikace běžných přístupových požadavků pro různé role zaměstnanců ve firmě ABC – například role konstruktéra, administrativního pracovníka nebo manažera. Každá z rolí vyžaduje přístup k jiným informacím a tyto potřeby je nutno identifikovat ještě před tvorbou prvních návrhů RBAC.

2. **Návrh modelu RBAC**

Druhým krokem je návrh modelu RBAC na základě rozboru z předchozího kroku, který mapuje role ve společnosti a s nimi svázaná přístupová oprávnění. Model by měl pokrývat všechny identifikované role, jejich potřeby a zároveň být dostatečně flexibilní k tomu, aby umožňoval jeho budoucí úpravy a změny specifikací.

3. **Implementace adresářových služeb**

Třetím krokem zlepšení procesu řízení přístupových oprávnění je implementace adresářových služeb, jakou je například Active Directory, pro centrální správu

uživatelských účtů, skupin a jejich oprávnění. Adresářové služby poskytují jednotné a jednoduché prostředí pro efektivní správu uživatelských přístupů, přičemž po jejich nasazení do provozu může být pole jejich působnosti dále rozšiřováno a využíváno k dalším účelům. Služby jako Active Directory umožňují efektivně spravovat a organizovat data o entitách v organizaci, což je pro potřeby Infosysu ideální.

#### **4. Definice přístupových politik**

Čtvrtým krokem je vytvoření přístupových politik v rámci adresářové služby z předchozího kroku. Přístupové politiky specifikují, které role mají přístup ke kterým adresářům a jaké akce mohou v těchto adresářích provádět. Nové politiky by se měly řídit modelem RBAC vytvořeným ve druhém kroku.

#### **5. Implementace RBAC**

Pátý krok je konfigurace oprávnění souborového systému na sdílených síťových discích Infosysu takovým způsobem, aby byly v souladu s přístupovými politikami definovanými v předchozích krocích. Přiřazování oprávnění ke složkám musí být prováděno na základě rolí identifikovaných v modelu RBAC, nikoliv podle potřeb jednotlivých zaměstnanců.

#### **6. Školení a dokumentace**

Posledním krokem je zaškolení správce systému a dalších osob, které s oprávněními manipulují spolu s tvorbou náležité dokumentace. Koncovým uživatelům je potřeba nastínit, jak operuje systém RBAC. Dokumentace by měla popisovat přístupové politiky, postupy pro žádost o přístup a osvědčené postupy pro správu oprávnění. Dokumentaci je dále potřeba udržovat aktuální a přidávat do ní relevantní získané poznatky.

#### **7. Provoz, monitorování a audit**

Po provedení příprav a nasazení do provozu je třeba provádět údržbové aktivity. Je nutno pravidelně provádět posouzení přístupu pro zajištění toho, aby uživatelé měli odpovídající úroveň přístupu v souladu s jejich aktuálními pracovními rolmi a odpovědnostmi. Pokud je potřeba, nadbytečná oprávnění by měla být odstraněna a naopak ta chybějící doplněna.

Další nezbytnou údržbovou aktivitou je monitorování a auditování přístupu uživatelů, pomocí nichž je společnost ABC schopna zaznamenávat jakékoliv neoprávněné pokusy o získání či modifikaci informací nebo potenciální kybernetické hrozby.

Výše popsany postup je plně dostačující pro společnost s požadavky a velikostí ABC, avšak v případě, kdy management projeví zájem jít o krok dál, lze implementovat navíc i tato řešení pro zjednodušení práce se systémem. Je ale na uvážení vedení společnosti, zda jejich přidaná hodnota odpovídá pořizovacím nákladům a údržbě. V poslední kapitole 6 tyto kroky navíc nejsou uvažovány.

- **Automatizace poskytování uživatelských oprávnění**

Vývoj, koupě nebo využití existujících nástrojů k automatizaci procesu managementu uživatelských účtů a rolí na základě jejich pracovních funkcí, například propojením s HR systémem, přináší snížení pracnosti a chybovosti. Zároveň však vzhledem k velikosti společnosti a počtu zaměstnanců v současnosti

nasazení takového řešení není vysoká priorita a pravděpodobně by se vůbec nevyplatilo.

- **Poskytování služeb samoobsluhy pro požadavky na přístup**

Implementace samoobslužného portálu, kde uživatelé mohou požádat o udělení rolí dále sníží pracnost a chybovost, avšak stále vyžadují zásahy správce oprávnění. Nasazení takového systému v současném stavu také není pro firmu příliš výhodné.

Po implementaci systému správy oprávnění, jak je v sekci popsáno, je společnost schopna mnohem efektivněji spravovat přístupy k datům a odhalovat potenciální hrozby. V budoucnu společnost ABC může uvažovat i o posledních dvou zmíněných bodech, jenž posouvají automatizaci na vyšší úroveň, avšak v krátkodobém nebo střednědobém období implementovány s největší pravděpodobností nebudou.

### 5.2.3 Zavedení šifrování dat na disku

Stávající řešení nevyužívá vůbec žádného šifrování dat, i když je řada z nich velmi citlivá – ať už o zaměstnancích, klientech nebo produktech, viz sekce 5.1.3 která o hrozbě pojednává blíže.

Ač se zavedení šifrování na úrovni sdílených síťových disků jeví jako nejjednodušší řešení, nefungovalo by dobře s Infosysem. Ten je totiž schopen pracovat pouze s nezašifrovanými daty a náležité úpravy by znamenaly přepracování kritické funkcionality a velké množství práce pro tvůrce systému, kterou již v současnosti není ochoten provádět.

Jako další řešení se nabízí využití cloudových služeb, avšak kvůli smlouvám s dodavateli není společnost ABC oprávněna uchovávat citlivá data zákazníků na externích úložištích. Migrace do cloudu by sice výrazně usnadnila aktivity spojené s údržbou dat, ale hrozba právních důsledků je příliš velká a tento přístup pro firmu není možný.

Z provedených analýz vyplývá, že nejlepším řešením pro společnost ABC je nasazení prvku *Network Attached Storage* (dále pod zkratkou NAS[34]). NAS disk je flexibilní a nabízí klíčovou funkcionalitu, jakou je šifrování jak na úrovni souborů, tak na úrovni celého disku. NAS disky jsou dále schopny se připojit do sítě a s využitím protokolu TCP/IP bezpečně komunikovat i přes nezabezpečené sítě, což přidává na flexibilitě a umožňuje uchovávat citlivá data fyzicky oddělena od zbytku firemní IT infrastruktury.

Network Attached Storage disk může společnost ABC implementovat pomocí následujících kroků:

1. **Určení požadavků na nové řešení**

V první fázi je nutno zjistit jaký objem a typ dat bude společnost chtít uchovávat. Podle toho pak může zvolit odpovídající velikost disku a pokud možno i s ohledem na budoucí nárůst množství dat.

2. **Výběr optimálního řešení NAS**

V druhé fázi je třeba na základě definovaných specifikací vybrat z dodavateli nabízených možností tu, která je pro firmu ABC nejlepší. Nejdůležitějšími vlastnostmi jsou schopnost aplikovat šifrování na úrovni souborů i disku, velikost úložiště a rychlosti čtení a zápisu. Populárními a osvědčenými poskytovateli jsou například společnosti Synology[36], QNAP[35] a Western Digital[37].

### 3. Konfigurace NAS disků

Ve třetí fázi se aktivity týkají fyzického nasazení disků a jejich integrace do správy uživatelských oprávnění. Je třeba zvolit místo, typ připojení (nejlépe drátové kvůli stabilitě a rychlosti) a diskům poskytnout i náležitou fyzickou ochranu. Pomocí prohlížečového rozhraní pak může správce jednoduše integrovat řešení popsané v 5.2.2 například nástrojem Active Directory. Nakonec zbývá nastavení ochrany na úrovni souborů pomocí vestavěné funkcionality NAS prvků a lze uvažovat i o zašifrování celého disku pomocí programu Bitlocker[33], avšak v takovém případě již výrazně roste doba přístupu k datům na disku.

### 4. Migrace sdílených složek na NAS

Čtvrtým krokem je přesun samotných souborů na nově nasazený disk. K již nastavenému a zaběhlému procesu zálohování dat pak správce může využít i další vestavěné funkcionality k tvorbě záloh nebo použít některou z RAID konfigurací úložiště.

### 5. Zaškolení a provoz

Po úspěšném projektu nasazení NAS je třeba jej nadále udržovat stahováním aktualizací, monitoringem a auditem bezpečnosti. Školení pro zaměstnance by mělo jasně popisovat jak s disky pracovat, jaké jsou doporučené postupy a jakým akcím se vyhýbat v zájmu bezpečnosti dat.

S nasazením NAS úložiště si společnost ABC vypomůže jak v oblasti šifrování, tak tvorby záloh a zvyšování robustnosti dat například použitím RAID 1 konfigurace (zrcadlení dat).

#### 5.2.4 Vylepšení uživatelského rozhraní

Infosys je již letitý systém a jeho rozhraní podle toho vypadá. Řada sekcí není vůbec používána nebo je z ní používán jen malý zlomek implementované funkcionality. Z těchto důvodů UI obsahuje zbytečně mnoho prvků, které by šly beze ztráty vyškrtnout. Barevná paleta má také prostor pro zlepšení, poněvadž po delší práci s Infosys není příjemná pro oči a rychle je unavuje.

Při úpravě rozhraní by měla být věnována pozornost následujícím bodům:

1. Odstranění překlepů, nevhodných anglicismů a nemístného hůlkového písma (viz podsekcce 5.1.7).
2. Odstranění nepoužívaných tlačítek, sekcí a omezení počtu generovatelných dokumentů.
3. Volba příjemnější barevné palety rozhraní.
4. Přidání možnosti zvětšovat text záznamů a ovládacích prvků.
5. Přidání zabudované nápovědy.
6. Umožnit uživateli přímo v Infosys otevřít výkres.

Drobné úpravy znění textu nebo použitých barev bude tvůrce systému pravděpodobně ochoten provést za menší poplatek, avšak za komplexnější funkcionality již poplatky budou vyšší, nebo autor nebude mít vůbec zájem o jejich implementaci. Výsledek tedy bude záležet

nejen na vedení firmy ABC, ale i na vývojáři Infosysu.

Na základě předchozích zkušeností s největší pravděpodobností odmítne přidání nápovědy, proklik na výkres z Infosysu a možnost zvětšování text a obrázků, proto nejsou brány v potaz v ekonomickém vyhodnocení tohoto návrhu.

### 5.2.5 Zvýšení frekvence zálohování textových dat MS Access

Tento návrh, přímočarý a snadno proveditelný, reaguje na nedostatek odhalen a popsán v podsekcí 5.1.5. IT pracovník Infosysu tvoří zálohy textových dat v MS Access pouze jedenkrát ročně, přičemž zálohy vygenerovaných dokumentů vytváří každý měsíc. Pokud dojde k úpravě procesu pro MS Access data způsobem, aby probíhaly zároveň se zálohováním dokumentů, bude ABC mnohem lépe připravena na výpadky dat a schopna lépe reagovat v krizi. Jedná se o jednoduchý a nenákladný způsob, jak získat hodně přidávané hodnoty a ABC by jej měla využít.

### 5.2.6 Odvrácení dopadů neoprávněných zásahů do souborů

V aktuální verzi neexistuje žádná mechanika, která by zabráňovala zaměstnanci nahlédnout do souborů jiných zaměstnanců a dokonce je upravovat či mazat. Ač se to ještě jako problém v praxi neprojevilo, tvoří to nezanedbatelnou hrozbu (více o ní v podsekcí 5.1.1).

Komplexním řešením je vytvořit rozsáhlou sadu bezpečnostních a přístupových politik takovým způsobem, aby mohl se souborem manipulovat pouze jeden člověk. To ale jde proti implementaci RBAC popsané v podsekcí 5.2.2, v implementaci bezpečnostních politik by tak vznikl chaos a hlavní principy a přínosy pro jejich nasazení by tím byly negovány.

Existují ale dva jednoduché a nenákladné kroky, jak hrozbu minimalizovat:

#### 1. Zavedení verzování souborů

Operační systém Windows poskytuje vestavěnou funkcionalitu, která umožňuje uchovávat pozmeněné verze souborů. V případě bezpečnostního incidentu, kdy dojde k nevyžádaným úpravám souborů, je systém Windows schopen úpravy revertovat a následky krize odstranit. Verzování souborů funguje i v situaci, kdy je soubor uživatelem úplně smazán.

#### 2. Zavedení auditních stop v práci se soubory

Podobně jako u předchozího bodu verzování souborů, i tato funkcionalita tvorby auditních stop se nachází v prostředí operačního systému. Po jeho konfiguraci pak Windows automaticky tvoří zápisy jak o úspěšných, tak i neúspěšných pokusech o přístup k jednotlivým souborům či složkám.

Implementace popsaného řešení tak sice hrozbě úplně nezabraňuje, avšak v případě kdy dojde k bezpečnostnímu incidentu, bude velmi jednoduché se vrátit do požadovaného stavu a zjistit, kdo nebo co k incidentu vedlo. Nasazení dvou popsaných funkcionalit společně tvoří jednoduché, levné a mocné řešení.

## Kapitola 6

# Ekonomické vyhodnocení navržených řešení

V této kapitole je rozvedeno ekonomické vyhodnocení navržených řešení, která mají za cíl vylepšit situaci ve firmě ABC. Hlavním úkolem tohoto vyhodnocení je poskytnout objektivní pohled na očekávané náklady a přínosy spojené s implementací navrhovaných změn. Toto zhodnocení hraje důležitou roli při podpoře rozhodování managementu o alokaci zdrojů.

Následující sekce poskytnou bližší pohled na odhadované náklady, očekávané benefity a finanční analýzu, která pomůže lépe porozumět ekonomickému dopadu.

Kapitola staví na návrzích zlepšení ze sekce 5.2, kterými se zabývá z pohledu získané přidané hodnoty a vynaloženého úsilí pro jejich implementování.

### 6.1 Vyhodnocení očekávaných přínosů

Předpokládané přínosy navržených změn jsou klíčovým faktorem při posuzování jejich ekonomického odůvodnění. Tato sekce se zaměřuje na detailní zhodnocení očekávaných přínosů, které vyplývají z implementace navržených řešení společností ABC. Cílem tohoto vyhodnocení je nejen kvantifikovat finanční přínosy, ale také identifikovat další hodnoty, jako je zlepšení procesů a zvýšení efektivity.

První sekce kapitoly se věnuje finančně kvantifikovatelným přínosům jako jsou například ušetřené hodiny práce. Druhá sekce pak rozvádí nefinanční benefity – připravenost na krizi, snížení chybovosti a podobně.

#### 6.1.1 Vyhodnocení finančních přínosů

Implementací navržených zlepšení společnost dosáhne řady benefitů, které je ovšem obtížné přesně vyjádřit. Většina výhod funguje jako mitigace hrozeb a určit to, kolik firma ABC ušetří tím že pracuje v souladu s GDPR, je velmi obtížné. Podobně prakticky nelze dobře odhadnout, kolik společnost ušetří tím, že bude pravidelně zálohovat klíčová textová data z MS Access – v běžném provozu neušetří nic, avšak pokud by došlo k situaci, kdy ztratí celý rok citlivých dat, firmě ušetří miliony a zabrání tomu, aby se dostala do obrovských potíží.

Přesto existuje několik položek kde je přínos vyčíslitelný a ty popisuje tabulka 6.1.

Z tabulky plyne předpoklad, že společnost ABC zavedením navrhovaných změn může ušetřit náklady na zaměstnance ve výši 11 290 Kč měsíčně, přičemž největší úsporu tvoří nově

| Návrh zlepšení                        | Položka                                  | Ušetřený čas v hodinách měsíčně |                 | Částka v korunách |
|---------------------------------------|------------------------------------------|---------------------------------|-----------------|-------------------|
|                                       |                                          | Zaměstnanci                     | Správce systému |                   |
| Zavedení uživatelských skupin         | Urychlení přidávání oprávnění            | 0                               | 1,5             | 615               |
|                                       | Ušetření práce při nápravě chyb          | 0                               | 2               | 820               |
|                                       | Zefektivnění managementu přístupů        | 0                               | 2               | 820               |
|                                       | Urychlení onboardingu nových zaměstnanců | 1                               | 1               | 810               |
| Vylepšení uživatelského rozhraní      | Zjednodušení zaučování zaměstnanců       | 1                               | 0               | 400               |
|                                       | Urychlení práce                          | 4                               | 0,5             | 1805              |
| Odvrácení dopadů neoprávněných zásahů | Urychlení napravování chyb               | 13                              | 2               | 6020              |

Obrázek 6.1: Přehled finančních benefitů, které jednotlivé vylepšení přinášejí. Zdroj: vlastní zpracování.

zavedená možnost tvorby automatické historie souborů. Pro kalkulaci ušetřených peněz byly uvažovány hodinové náklady pro zaměstnance ve výši 400 Kč za hodinu práce a pro správce systému 410 Kč za hodinu.

### 6.1.2 Vyhodnocení nefinančních přínosů

Navržené vylepšení přináší řadu výhod, které lze jen obtížně vyjádřit přesnou částkou. Výčet vylepšení a přínosů, které z nich plynou, popisuje tabulka 6.2.

Ze seznamu přínosů lze vyčíst, že většina návrhů je orientována spíše jako prevence hrozeb nebo snížení jejich dopadů. Jejich přidaná hodnota se nejvíce projeví až ve chvíli, kdy nastane s nimi spojená krize a zafungují jako mitigace.

## 6.2 Vyhodnocení očekávaných nákladů

V následující sekci kapitoly vyhodnocení jsou vyčísleny očekávané náklady implementace jednotlivých návrhů pro zlepšení a zaznamenány v tabulce 6.3. Pro kalkulaci mzdových nákladů byly uvažovány hodinové náklady pro management ve výši 480 Kč za hodinu práce, pro správce systému 410 Kč a pro konstruktéry částka 400 Kč za hodinu. Ti se sice v tabulce neobjevují, avšak náklady s nimi spojené figurují v položkách školení, kterých se zúčastní. Částka pořízení NAS disku byla zvolena orientačně pro disky určené malé a střední podniky se základní funkcionalitou. Z tabulky lze vyčíst, že náklady pro implementaci navržených vylepšení dostahují částky 118 070 Kč, přičemž vyžadují dalších 7 405 Kč měsíčně.

| Návrh zlepšení                             | Přínos                                                                    |
|--------------------------------------------|---------------------------------------------------------------------------|
| Úprava firemních procesů v souladu s GDPR  | Mitigace hrozby právních problémů                                         |
|                                            | Příprava na potenciální krizi úniku dat                                   |
| Zavedení uživatelských skupin              | Snížení chybovosti přidělování práv                                       |
|                                            | Mitigace hrozby ponechání nadbytečných pravomocí                          |
|                                            | Lépe škálovatelný způsob managementu přístupů                             |
| Zavedení šifrování dat na disku            | Významné zvýšení bezpečnosti dat                                          |
|                                            | Zábrana zneužití dat v případě zcizení úložišť                            |
| Vylepšení uživatelského rozhraní           | Jednodušší uživatelské rozhraní                                           |
|                                            | Lepší user experience pro zaměstnance                                     |
| Zvýšení frekvence zálohování dat MS Access | Snížení dopadů ztráty citlivých dat                                       |
| Odvracení dopadů neoprávněných zásahů      | Schopnost auditovat aktivity zaměstnanců                                  |
|                                            | Možnost vracet se ke starším verzím souborů i v případě kdy dojde k omylu |

Obrázek 6.2: Přehled nefinančních benefitů, které jednotlivé vylepšení přinášejí. Zdroj: vlastní zpracování.

| Návrh zlepšení                             | Položka                                    | Potřebný čas v hodinách |                 | Částka v korunách |
|--------------------------------------------|--------------------------------------------|-------------------------|-----------------|-------------------|
|                                            |                                            | Management              | Správce systému |                   |
| Úprava firemních procesů v souladu s GDPR  | Audit a klasifikace dat                    | 3                       | 12              | 6360              |
|                                            | Konzultace s právníkem                     | 0                       | 0               | 20000             |
|                                            | Tvorba krizového plánu                     | 9                       | 9               | 8010              |
|                                            | Provoz, audit                              | 2 měsíčně               | 7 měsíčně       | 3830              |
| Zavedení uživatelských skupin              | Rozbor aktuálních přístupových požadavků   | 1                       | 11              | 4990              |
|                                            | Návrh modelu RBAC                          | 2                       | 10              | 5060              |
|                                            | Nasazení Active Directory                  | 0                       | 17              | 6970              |
|                                            | Implementace RBAC modelu                   | 0                       | 5               | 2050              |
|                                            | Školení uživatelů                          | 3                       | 1               | 6250              |
|                                            | Tvorba dokumentace                         | 1                       | 4               | 2120              |
|                                            | Provoz, audit                              | 0                       | 5 měsíčně       | 2050              |
| Zavedení šifrování dat na disku            | Identifikace požadavků na nové řešení      | 1                       | 6               | 2940              |
|                                            | Výběr optimálního NAS disku                | 1                       | 11              | 4990              |
|                                            | Pořízení NAS disku                         | 0                       | 0               | 12000             |
|                                            | Konfigurace a nasazení NAS disku           | 0                       | 32              | 13120             |
|                                            | Školení                                    | 3                       | 1               | 6250              |
|                                            | Provoz                                     | 0                       | 4 měsíčně       | 1640              |
|                                            | Odstranění překlepů a drobné úpravy        | 0                       | 0               | 1000              |
| Vylepšení uživatelského rozhraní           | Odstranění nepoužívaných tlačítek          | 0                       | 0               | 4000              |
|                                            | Odstranění nepoužívaných dokumentů         | 0                       | 0               | 3500              |
|                                            | Změna barevné palety rozhraní              | 0                       | 0               | 6000              |
| Zvýšení frekvence zálohování dat MS Access | Čas samotného zálohování                   | 0                       | 0,5 měsíčně     | 205               |
| Odvrácení dopadů neoprávněných zásahů      | Zavedení verzování souborů                 | 0                       | 2               | 820               |
|                                            | Zavedení auditních stop v práci se soubory | 0                       | 4               | 1640              |

Obrázek 6.3: Přehled očekávaných nákladů. Sloupec s částkou zahrnuje jak náklady na mzdy, tak fixní náklady. Zdroj: vlastní zpracování.

# Kapitola 7

## Závěr

Cílem této diplomové práce je provést analýzu současného stavu informačního systému společnosti ABC, zhodnotit jeho vlastnosti a navrhnout opatření k vylepšení aktuálního stavu systému.

V teoretické části práce jsou vysvětleny základní pojmy z oblasti informačních systémů, včetně architektury IS, jejich klasifikace nebo životního cyklu. Dále jsou popsány analytické nástroje, jakými jsou PEST a Porterova analýza pěti sil, včetně použité hodnotící metody ZEFIS. Teoretická část se věnuje i tématům uživatelských rozhraní, user experience a bezpečnosti. Na těchto předdefinovaných poznatcích pak staví zbytek diplomové práce.

Analytická část práce se zaměřuje na představení anonymizované společnosti ABC a jejího zkoumaného informačního systému Infosys. Následuje analýza vnějšího prostředí pomocí PEST a Porterova modelu spolu s analýzou samotného informačního systému metodou ZEFIS.

Návrhová část práce navazuje na analytickou část a poznatky, které přinesla. Zaměřuje se na zvýšení zabezpečení informačního systému firmy a zvýšení efektivity správy uživatelských oprávnění. Na základě získaných dat z předchozích analýz je navrženo šest opatření, která výrazně zlepší informační bezpečnost ve společnosti. Opatřeními jsou šifrování disků, zavádění uživatelských skupin podle modelu RBAC, předcházení právním GDPR hrozbám, mitigace dopadů sabotérské činnosti zaměstnanců, vylepšení uživatelského rozhraní Infosysu a zlepšení procesu zálohování klíčových dat.

Na závěr jsou provedena ekonomická zhodnocení finančních i nefinančních přínosů spolu s výpočtem očekávaných nákladů. Z této kapitoly vyplývá, že navržená opatření s sebou nenesou vysoké náklady a několik z nich je snadné implementovat. Jejich přidanou hodnotou je jednak úspora hodin práce, ale důležitější je eliminace nebo snížení velkých hrozeb, se kterými se firma ABC může v budoucnu potýkat. Výstupem práce jsou tedy úpravy menšího rázu, které pomáhají předejít velkým problémům.

# Literatura

- [1] *American National Standards Institute - ANSI Home* [online]. 2023 [cit. 2024-03-11]. The American National Standards Institute oversees standards and conformity assessment activities in the United States. Dostupné z: <https://www.ansi.org/>.
- [2] BASL, J. a BLAŽIČEK, R. *Podnikové informační systémy: podnik v informační společnosti*. 3., aktualizované a doplněné vydání. Praha: Grada, 2012. ISBN 978-80-247-4307-3.
- [3] CANZIBA, E. *Hands-on UX Design for Developers: Design, Prototype, and Implement Compelling User Experiences from Scratch*. 1st edition. Birmingham, UK: Packt Publishing, 2018. ISBN 978-1-78862-669-9.
- [4] *Nárůst cen energií od roku 2021* [online]. 2024 [cit. 2024-04-07]. Dostupné z: <https://www.consilium.europa.eu/cs/infographics/energy-prices-2021/>.
- [5] CHECKLAND, P. a SCHOLLES, J. *Soft Systems: Methodology in Action*. 1. vyd. New York: John Wiley, 1996. ISBN 0-471-92768-6.
- [6] *Standard C++* [online]. 2024 [cit. 2024-04-18]. Dostupné z: <https://isocpp.org/>.
- [7] *Inflace, spotřebitelské ceny* [online]. 2024 [cit. 2024-04-07]. Dostupné z: [https://www.czso.cz/csu/czso/inflace\\_spotrebitelske\\_ceny](https://www.czso.cz/csu/czso/inflace_spotrebitelske_ceny).
- [8] *Šetření průměrných cen vybraných výrobků - pohonné hmoty a topné oleje - časové řady* [online]. 2024 [cit. 2024-04-07]. Dostupné z: <https://www.czso.cz/csu/czso/setreni-prumernych-cen-vybranych-vyrobku-pohonne-hmoty-a-topne-oleje-casove-rady>.
- [9] *Compliance FAQs: Federal Information Processing Standards (FIPS)* [online]. 2019 [cit. 2024-03-11]. List of current FIPS standards with links to the files. Dostupné z: <https://www.nist.gov/standardsgov/compliance-faqs-federal-information-processing-standards-fips>.
- [10] HANÁČEK, P. a STAUDEK, J. *Bezpečnost informačních systémů: metodická příručka zabezpečování produktů a systémů budovaných na bázi informačních technologií*. Praha: Úřad pro státní informační systém, 2000. ISBN 80-238-5400-3.
- [11] *IEEE SA - The IEEE Standards Association - Home* [online]. 2024 [cit. 2024-03-11]. Raising the World's Standards. Dostupné z: <https://standards.ieee.org/>.
- [12] *IETF / RFCs* [online]. 2024 [cit. 2024-03-11]. Internet standards RFCs. RFC documents contain technical specifications and organizational notes for the Internet. RFCs produced by

the IETF cover many aspects of computer networking. They describe the Internet's technical foundations, such as addressing, routing, and transport technologies. Dostupné z: <https://www.ietf.org/standards/rfcs/>.

- [13] *Informačně bezpečná Praha 2*. 2024 [cit. 2024-03-11]. Náskres souvislostí v informační bezpečnosti. Dostupné z: <https://www.expinit.cz/novinky/informacne-bezpecna-praha-2>.
- [14] JOHNSON, G. a SCHOLLES, K. *Exploring Corporate Strategy*. 4th ed. London: Prentice Hall, 1997. ISBN 0-13-525635-6.
- [15] KEŘKOVSKÝ, M. *Strategické řízení: teorie pro praxi*. 2. vyd. Praha: C. H. Beck, 2002. ISBN 978-807-1795-780.
- [16] KOCH, M. *Zefis – Audit informačních systémů, portál Ústavu informatiky Fakulty podnikatelské VUT v Brně* [online]. 2024. Cit. 2024-02-12. Dostupné z: <http://zefis.cz/>.
- [17] KOCH, M., NENIČKOVÁ, H., HRŮZA, T. a DOVRTĚL, J. *Management informačních systémů*. 3rd, revised. Brno: Akademické nakladatelství CERM, 2010. ISBN 978-80-214-4157-6.
- [18] KONEČNÝ, V. *Projektování informačních systémů*. Vyd. 1. Brno: Mendelova zemědělská a lesnická univerzita, 1996. ISBN 80-7157-241-1.
- [19] KUHLEN, R. Information and pragmatic value-adding: Language games and information science. *Computers and the Humanities*. Leden 1991, sv. 25. DOI: 10.1007/BF00124146.
- [20] KUMAR, R. R. *Human Computer Interaction*. 2nd edition. New Delhi: Laxmi Publications, 2005. ISBN 9788170087953.
- [21] LAUESEN, S. *User Interface Design: A Software Engineering Perspective*. Původní vydání. Harlow, England: Pearson/Addison-Wesley, 2005. ISBN 0-321-18143-3.
- [22] MOLNÁR, Z. *Efektivnost informačních systémů*. 2. rozšířené vydání. Praha: Grada, 2001. ISBN 80-247-0087-5.
- [23] *Databázový software a aplikace / Microsoft Access* [online]. 2024 [cit. 2024-04-18]. Dostupné z: <https://www.microsoft.com/cs-cz/microsoft-365/access>.
- [24] ONDRÁK, V. *Management informační bezpečnosti*. Brno: Vysoké učení technické v Brně, 2014.
- [25] JONSSON, J. a KALISKI, B. *Public-Key Cryptography Standards (PKCS) no. 1: RSA Cryptography Specifications Version 2.1* [online]. 2003 [cit. 2024-03-11]. Informational RFC, February 2003. Dostupné z: <https://datatracker.ietf.org/doc/rfc3447/>.
- [26] POUR, J. *Informační systémy a elektronické podnikání*. Vyd. 1. Vysoká škola ekonomická, Fakulta informatiky a statistiky, 2001. ISBN 80-245-0227-5.
- [27] *Qt / Tools for Each Stage of Software Development Lifecycle* [online]. 2024 [cit. 2024-04-18]. Dostupné z: <https://www.qt.io/qt-examples-for-webassembly>.

- [28] SEDLÁČKOVÁ, H. a BUCHTA, K. *Strategická analýza*. 2., přepracované a doplněné vydání. Praha: C.H. Beck pro praxi, 2006. ISBN 8071793671.
- [29] SKLENÁK, V. *Data, informace, znalosti a Internet*. Vyd. 1. Praha: Nakladatelství C H Beck, 2001. ISBN 80-7179-409-0.
- [30] SODOMKA, P. a KLČOVÁ, H. *Informační systémy v podnikové praxi*. 2. aktualizované a rozšířené vydání. Brno: Computer Press, 2010. ISBN 978-80-251-2878-7.
- [31] TVRDÍKOVÁ, M. *Aplikace moderních informačních technologií v řízení firmy: nástroje ke zvyšování kvality informačních systémů*. 1. vyd. Praha: Grada, 2008. ISBN 978-80-247-2728-8.
- [32] *What Is UX Design?* [online]. 2024 [cit. 2024-04-09]. Dostupné z: <https://bootcamp.cvn.columbia.edu/blog/what-is-ux-design/>.
- [33] *Bitlocker overview – Windows Security / Microsoft Learn* [online]. 2024 [cit. 2024-04-29]. Dostupné z: <https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/>.
- [34] *What Is Network Attached Storage (NAS)? / IBM* [online]. 2024 [cit. 2024-04-29]. Dostupné z: <https://www.ibm.com/topics/network-attached-storage>.
- [35] *QNAP / Odborníci na NAS, síť a chytré dozorování* [online]. 2024 [cit. 2024-04-29]. Dostupné z: <https://www.qnap.com/cs-cz>.
- [36] *Synology Inc.* [online]. 2024 [cit. 2024-04-29]. Dostupné z: <https://www.synology.com/en-global>.
- [37] *Network Attached Storage (NAS) / Western Digital* [online]. 2024 [cit. 2024-04-29]. Dostupné z: [https://www.westerndigital.com/solutions/network-attached-storage?filterByColor\\_List=Red%7CFF0000](https://www.westerndigital.com/solutions/network-attached-storage?filterByColor_List=Red%7CFF0000).
- [38] *WineHQ - Run Windows applications on Linux, BSD, Solaris and macOS* [online]. 2024 [cit. 2024-04-18]. Dostupné z: <https://www.winehq.org/>.
- [39] *What Is Backup? How Often Should You Backup Data?* [online]. 2024 [cit. 2024-04-30]. Dostupné z: <https://www.g2.com/articles/what-is-backup>.
- [40] *ZEFIS – audit informačních systémů* [online]. 2024 [cit. 2024-03-24]. Dostupné z: <https://www.zefis.cz/index.php?p=21>.
- [41] *Úřad pro ochranu osobních údajů*. 2024 [cit. 2024-03-31]. Webové stránky Úřadu pro ochranu osobních údajů. Dostupné z: <https://uoou.gov.cz/>.