

Západočeská univerzita v Plzni

Fakulta aplikovaných věd

Katedra informatiky a výpočetní techniky

Analýza rizik podnikových informačních systémů

Plzeň, 2014

Dominik Mirovský

Prohlášení

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně a výhradně s použitím citovaných pramenů.

V Plzni dne 7. 4. 2014

.....

Dominik Mirovský

Poděkování

Děkuji vedoucí bakalářské práce Doc. Dr. Ing. Janě Klečkové za cenné rady při vedení práce a doporučení zdrojů, ze kterých čerpat.

Abstract

Risk analysis of enterprise information systems

The main concern of this thesis are information systems and risks associated with them. The work is based on the staged theory, which is explained in detail. By taking up knowledge of the staged theory, we were able to analyze risks of the information systems associated with GlaxoSmithKline Ltd., one of the largest pharmaceutical companies in the world. The theoretical part of the thesis deals with general issues of risk information systems and individual analysis. In the practical part, financial analysis is made first and then risk analysis of information systems. Company assets, the threats affecting them and the resulting risks were determined. In the conclusion of the thesis, possible security measures to protect company assets were proposed.

Abstrakt

Analýza rizik podnikových informačních systémů

Hlavní náplní této práce je problematika informačních systémů a rizika s nimi spojená. Z nastudovaných materiálů je podrobně vylíčen přechod z popsané teorie do praxe. Teoretická část se zabývá obecnou problematikou rizik informačních systémů a jednotlivým analýzám. V praktické části je pak uskutečněná nejprve finanční analýza farmaceutické firmy GlaxoSmithKline s.r.o., z důvodu zjištění finanční stability firmy a poté analýza rizik jejích podnikových informačních systémů. V průběhu analýzy se stanovila aktiva firmy, poté na ně působící hrozby a na konec se vypočítala rizika působící na jednotlivá aktiva. V závěru se pak stanovil jakýsi přehled bezpečnostních opatření, která mají za úkol chránit aktiva firmy.

Obsah

| | |
|--|----|
| Prohlášení | 2 |
| Poděkování..... | 3 |
| Abstract..... | 4 |
| Abstrakt..... | 4 |
| 1. Úvod..... | 1 |
| 2. Vymezení pojmu informační systém | 1 |
| 2.1. Podnikové informační systémy | 2 |
| 2.2. Lidé | 2 |
| 2.3. Zavedení IS do podniku | 2 |
| 2.4. Chyby při zavádění IS do podniku | 3 |
| 2.5. Inovace | 4 |
| 3. Rizika Informačních systémů | 4 |
| 3.1. Metody analýzy rizik | 5 |
| 3.2. Kvalitativní metody | 5 |
| 3.2.1 Metoda účelových interview | 5 |
| 3.3. Kvantitativní metody..... | 7 |
| 3.3.1 Metoda CRAMM (Risk Analysis and Management Methodology)..... | 7 |
| 4. Finanční analýza..... | 7 |
| 4.1. Elementární metody finanční analýzy..... | 8 |
| 5. Analýza rizik informačních systémů vybrané společnosti | 14 |
| 5.1. Identifikace aktiv | 15 |
| 5.2. Ohodnocení aktiv | 15 |
| 5.3. Podnikové informační systémy | 16 |

| | | |
|-------|---|----|
| 5.3.1 | SUNsystems | 17 |
| 5.3.2 | CITIBANK | 18 |
| 5.3.3 | EPOS..... | 18 |
| 5.3.4 | TREX | 19 |
| 5.3.5 | HELIOS..... | 20 |
| 5.3.6 | ARCHA | 20 |
| 5.4. | Realizace finanční analýzy | 21 |
| 5.4.1 | Výsledky: | 22 |
| 5.5. | Riziko investice do informačních systémů | 28 |
| 5.6. | Riziko výpadku informačního systému..... | 29 |
| 5.7. | Ohodnocení případných škod dopadu na aktiva | 30 |
| 5.8. | Zařazení aktiv do pásem..... | 31 |
| 6. | Hrozby..... | 32 |
| 6.1. | Identifikace hrozeb..... | 32 |
| 6.1.1 | Rozdělení hrozeb podle možnosti vzniku | 33 |
| 6.1.2 | Vyplnění tabulek | 34 |
| 6.2. | Hodnocení hrozeb | 34 |
| 7. | Rizika | 36 |
| 7.1. | Hodnocení rizik..... | 36 |
| 8. | Bezpečnostní opatření | 41 |
| 8.1. | Navrhovaná opatření pro jednotlivá rizika | 41 |
| 8.1.1 | Požár a výpadek elektrického proudu | 41 |
| 8.1.2 | Chyba správce, chyba uživatele | 41 |
| 8.1.3 | Kyberterorismus | 42 |
| 8.1.4 | Odposlouchávání | 42 |

| | | |
|-------|---|----|
| 8.1.5 | Použití škodlivého softwaru..... | 42 |
| 8.1.6 | Selhání softwaru, selhání hardwaru, selhání sítě..... | 43 |
| 9. | Závěr | 44 |
| | Seznam použitých zdrojů:..... | 46 |

1. Úvod

Cílem této práce je provedení analýzy rizik podnikových informačních systémů vybraného podniku.

Obsah práce se rozděluje na dvě části – část teoretickou a část praktickou. Tyto dvě části jsou od sebe logicky oddělené. První z nich obsahuje načerpané znalosti zkoumané problematiky a druhá je využitím těchto znalostí v řešené úloze.

V teoretické části je nejprve vymezen pojem informační systém a jeho využití v praxi. Zároveň se ale také zabývá rozvojem informačního systému, který stále významněji ovlivňuje globální charakter společnosti. Je zde také uveden význam tohoto pojmu pro podniky, protože právě v tomto odvětví mají informační systémy nejširší využití. Podnikům tyto systémy pomáhají dosáhnout jejich cílů.

V praktické části je pak provedena analýza rizik podnikových informačních systémů konkrétní firmy. Tato analýza vychází nejprve z přiblížení finanční stability podniku, dále je analýza provedena na základě načerpaných znalostí popsaných v teoretické části práce a dostupnosti relevantních dat.

2. Vymezení pojmu informační systém

Pro definování pojmu informační systém (IS) je velmi důležité objasnění obsaženého pojmu, tedy informace a také pojmu data.

Pojem data je definován jako vyjádření skutečnosti, která je schopná uchování, nebo dalšího přenosu, interpretace a zpracování. Příkladem jsou tedy posloupnosti prvků, symbolů, hodnot a veličin. Jsou to základní stavební veličiny informace, viz [12], [13].

Od zakladatele kybernetiky, Norberta Wienera, je známo, že informace je nehmotné povahy, viz [1]. Později tuto myšlenku doplnilo bádání a nabyté zkušenosti dalších významných osobností, zabývajících se touto problematikou. Podle jedné z neexaktních definic je informace pravděpodobnost výskytu znamení nebo signálu, který eliminuje neznalost příjemce. Tato definice je však pro hloubku této práce

nedostačující. Mnohem hlubší charakter má definice založená na vědomí, že lidé chápou informaci jako nepostradatelnou součást rozhodování, ať už v osobním životě nebo podnikání. Informace jsou tak nezbytnou součástí pro vymezení a pochopení, co to IS je, viz [1].

Definice IS totiž pevně stojí na způsobu, jak lidé za pomoci technologických prostředků a metod shromažďují, zpracovávají a uchovávají data tak kvalitně, aby bylo možné vytvořit z nich informace sloužící pro potřeby uživatelů, viz [1].

2.1. Podnikové informační systémy

Podnikový informační systém je vlastně soubor aplikací, které slouží ke sběru a ukládání dat, jejich následné zpracování, vyhodnocování, předávání mezi pracovníky a jejich výměnu s partnery a klienty. I když je výhodné mít většinu dat uloženu v jednotném informačním systému, nejlépe od jednoho dodavatele, v praxi to obvykle není možné a podnikové informační systémy se skládají běžně například ze systému elektronické pošty, systému pro správu a oběh dokumentů, systém pro správu výkresové dokumentace, ekonomický a účetní systém, systém pro servis, systém pro řízení vztahů se zákazníky (CRM) a nejrůznější další, dle toho v jakém oboru firma podniká, viz [3].

2.2. Lidé

Tento pojem vysvětluje následující definice: *Podnikový informační systém vytvářejí lidé, kteří prostřednictvím dostupných technologických prostředků a stanovené metodologie zpracovávají podniková data a vytvářejí z nich informační a znalostní bázi organizace sloužící k řízení podnikových procesů, manažerskému rozhodování a správě podnikové agendy*, viz [1]. Tato definice se nezmiňuje o prvku automatizace, tedy přítomnosti softwaru nebo hardwaru, protože tyto prvky jsou bez lidí, kteří je řídí zanedbatelné. Nejdůležitější je rozhodování lidí a činnosti vedoucí podnik směrem dopředu.

2.3. Zavedení IS do podniku

Úkolem lidí, v tomto případě podnikových manažerů, je také umění efektivního zavedení daného IS do podniku a jeho maximální využití. Účelem IS v podniku je sice

zefektivnění výroby a přínos vyšších zisků, nicméně těžko takových výsledků dosáhnout, jestliže systém přesně „nesedí“ ke koncepci daného podniku. IS v podniku musí mít dynamický charakter a umět se přizpůsobit nejrůznějším situacím. V každém podniku nastávají odlišné situace a musí se řešit jiné problémy. Klíčem úspěchu je tedy přednostní definování cílů podniku a poté nasazení adekvátního druhu IS, podle autora knihy Petra Sodomky, dle následujících kroků, viz [1]:

- *Specifikovat řešené problémy na základě analýzy stávajícího stavu a požadavků organizace.*
- *Stanovit cíle a naplánovat realizaci projektu, včetně analýzy využití pokročilých metod návrhu IS.*
- *Naplánovat novou koncepci řízení IS, a to v návaznosti na hodnocení efektivnosti řízení stávající koncepce.*

Jakýkoli jiný přístup je prý nežádoucí a velmi riskantní, viz [1].

Při implementaci podnikového IS se doporučuje týmová koordinace a spolupráce. Jeden pracovník pak může kontrolovat druhého a obráceně. V praxi se tento systém týmové implementace osvědčil. Každý z pracovníků musí být schopen vykonávat veškerou práci samostatně, ale jde především o efektivitu a časovou náročnost, kvůli kterým se týmová práce vyplatí. Důležitá je komunikace ve smyslu otevřenosti vůči ostatním spolupracovníkům. Je důležité, aby se jednotliví členové týmu znali osobně a co nejrychleji tak bez komunikačních bariér postupovali k danému cíli, viz [1].

2.4. Chyby při zavádění IS do podniku

Nejčastější nebo lépe řečeno největší chybou při zavádění IS do podniku jako ekonomického subjektu je vznik nadbytečně vysokých nákladů. Náklady nezbytné na implementaci IS přesahují často rámec v momentě, kdy si zákazník neumí jasně stanovit požadavky. Nastává pak situace zpětného řešení problémů ze strany dodavatele a dalších úprav, které by při lepší prvotní komunikaci nevznikly, přičemž náklady pochopitelně rostou. Chyba může samozřejmě nastat také na straně dodavatele, proto je komunikace velmi důležitá a neměla by se podceňovat, viz [2], [11].

Dá se tedy říci, že jako chybový faktor v podniku působí hlavně lidé, i když je to v jistém rozporu s bodem 2.2. Lidé podnik řídí a řídí také IS, proto po celou dobu života podniku dochází k chybám způsobeným lidským faktorem.

Důležité je také uvědomit si, že zavedením IS do podniku nezaniká vztah dodavatele a zákazníka, ale naopak často vzniká bod počátku budoucí spolupráce. IS je třeba neustále inovovat a dodavatel musí také počítat, že zákazník bude potřebovat stále rozšiřovat schopnost sběru informací a efektivní chod podniku. Rozšiřuje-li se podnik, rozšiřuje se také informační systém, viz [1].

Pokud informační systém přestane dostáčet potřebám organizace nebo se management při plánování IT projektu dopustí vážných chyb, pak je třeba učinit obtížné rozhodnutí o reengineeringu projektu, které může také znamenat ztrátu investic. Praxe ukazuje, že překonat tuto fázi je nesmírně obtížné. Pokračování v "nikdy nekončící implementaci" nevhodného produktu s nevhodným partnerem však přinese v konečném důsledku daleko větší ztráty, viz [1].

2.5. Inovace

Dalším důležitým faktorem pro rozvoj podniku jsou inovace. Je to vlastně řešení problémů, které se v podniku vyskytnou jiným, dalším způsobem. Neinovují se ale pouze oblasti podniku, které jsou nejslabšími články, a tudíž se na ně vztahuje nejvyšší pozornost inovátorů, ale na veškeré podnikové dění. Neustále inovovaný podnik získává náskok před konkurencí a zvyšuje se jeho potenciál růstu. Inovátorství dokáže podniku přinést jednu z klíčových rolí - takový podnik se totiž stane často známým a zákazníci vždy raději sáhnou po osvědčené značce, která jde s dobou. Inovace podniku bezesporu také znamená inovaci IS. To si vyžaduje spolupráci s nejnovějšími technologiemi, které dnešní doba poskytuje ve stále rostoucí míře, viz [2].

3. Rizika Informačních systémů

Riziko je možnost nežádoucího stavu, do kterého se podnik může souladem určitých okolností dostat. Tento stav však většinou není nečekanou událostí, protože firma "bez rizik" neexistuje. Každý podnik neustále podstupuje určitá rizika nebo se alespoň blíží

k jejich vzniku. Úkolem firmy, která chce prosperovat je neutíkat před otázkou určitého rizika nebo se rizikům snažit jakkoli vyhnout, ale brát je jako součást přirozeného běhu firmy a umět je řídit, viz [4].

Podle Prof. Jiřího Voříška je nasazování IS do podniku velmi rizikovou záležitostí. Tvrdí, že Informační systémy a informační technologie jsou sice velmi významným faktorem hospodářského prostředí, ale pozitivní efekt nepřinášejí zcela automaticky. Naopak řada informatických projektů skončila neúspěšně a přinesla jejich investorům nemalé ztráty. Popisuje pak ve své práci jednotlivé kritické faktory úspěchu a rizika informačních systémů, viz [11].

3.1. Metody analýzy rizik

Pro analýzu se využívá speciálních soborů metod. Metody lze rozdělit do dvou základních skupin:

1. Kvalitativní metody
2. Kvantitativní metody

K analýze se používá buď jeden typ metod, nebo kombinace obou přístupů, viz [4].

3.2. Kvalitativní metody

Rizika pomocí těchto metod jsou vyjádřena v určitém rozsahu, například bodováním podle čísel, či intervalem pravděpodobnosti. Hodnoty se určují kvalifikovaným odhadem. Tyto metody jsou jednodušší a časově méně náročné, než kvantitativní metody, viz [4].

3.2.1 Metoda účelových interview

Nejčastěji používanou kvalitativní metodou je metoda účelových interview nebo také metoda Delphi. Tato metoda vyžaduje spolupráci mezi experty provádějícími analýzu a schopnými představiteli podniku, kterého se analýza týká. Spolupráce spočívá v řízených rozhovorech, při kterých experti hodnotící skupiny kladou představitelům firmy předem vypracované otázky, na které respondenti jednotlivě odpovídají. Druhou formou může být hromadné vyplňování elektronických dotazníků. Pohovory probíhají jednotlivě, aby se příslušníci hodnocené organizace navzájem neovlivňovali. Obvykle

probíhají dvě až tři kola pohovorů, přičemž po každém kole probíhá shrnutí zodpovězených otázek. Z nich vypracované výsledky jsou opět předloženy respondentům za účelem potvrzení, či úpravy jejich stanovisek pro výsledný efekt. Výhodou metody je minimální časová náročnost, viz [4].

V praxi se využívají kvalitativní metody tabulkových formulářů, do kterých se v průběhu rozhovorů zaznamenávají data.

Použití kvalitativní metody v praxi:

- Prvním krokem je identifikace podnikových aktiv.

Aktivny se rozumí vše co má pro společnost nějakou hodnotu, což mohou být v rámci analýzy rizik IS například hardware, nebo software. Takto nalezená aktiva, se ohodnotí číselně od 1 do 9. Číslem 1 se ohodnotí nejméně hodnotná aktiva a číslem 9 aktiva, která mají pro podnik největší hodnotu, viz [4].

- Poté je na řadě identifikace hrozeb.

Druhým bodem je identifikace hrozeb. Pro identifikovaná aktiva se určí pravděpodobné hrozby a zapíše se do příslušné tabulky. Jako příklad si uvedme selhání softwaru, které může být pro podnik klíčovou hrozbou. Opět se hodnotí číselnými údaji, viz [4].

- Následuje vytvoření matice.

Do matice se doplní hrozby spolu s jejich pravděpodobností a aktiva s vyčíslenou hodnotou. Jako další krok přichází posouzení zranitelností jednotlivých aktiv. Takto vznikne matice zranitelností. Jestliže mezi aktivem a hrozbou žádná vazba neexistuje, tak zůstane buňka prázdná, viz [4].

Posledním krokem je vytvoření a doplnění druhé matice, tedy matice rizik. Tato matice vypadá stejně jako matice zranitelností, avšak obsahuje jiné hodnoty. Matice udává míru rizika. K výpočtu míry rizika slouží vztah:

$$R = T * A \quad (3.2.1)$$

kde „R“ představuje míru rizika, T představuje pravděpodobnost vzniku hrozby a „A“ je hodnota aktiva. Podle tohoto vzorce je vypočtena míra rizika a doplněna do matice. Nyní už zbývá pouze určit, jak jsou jednotlivá rizika klíčová. Rizika tedy rozdělíme podle hodnot na vysoká, střední a nízká rizika, viz [4].

3.3. Kvantitativní metody

Metody kvantitativní jsou založené na matematickém výpočtu podle počtu výskytu hrozeb a míry jejich dopadu. Na rozdíl od kvalitativních metod vyjadřují míru rizika ve finančních jednotkách, tedy korunách. Nejčastěji se pak uvádí předpokládaná roční ztráta. Vypracování těchto metod je logicky časově náročnější, avšak výsledky jsou lépe uchopitelné a mají větší význam. Tyto metody slouží především v oblasti bezpečnosti podniků a jejich informačních systémů, viz [4].

3.3.1 Metoda CRAMM (Risk Analysis and Management Methodology)

Metoda CRAMM je nejnámějším typem kvantitativní metody. V této metodě se postupně seskupí podniková aktiva do logických skupin, poté se aktiva ohodnotí a stanoví se hrozby, které skupiny ovlivňují. Tím se z bezpečnostního hlediska prozkoumá celý systém fungování společnosti a identifikují se nejzranitelnější místa. Na základě vzniklého modelu se stanoví požadavky na bezpečnost a aplikují se potřebná opatření. Data jsou zprostředkována prostřednictvím pohovorů mezi pracovníky podniku a experty hodnotící skupiny. Nevýhodou metody je její vysoká finanční náročnost, viz [4].

4. Finanční analýza

Finanční analýzu lze zařadit jako součást analýzy rizik proto, abychom posoudili schopnost financovat pořízení a provoz IS. Neschopnost subjektu financovat pořízení a provoz IS může vést k nárůstu rizik vzniklých v důsledku ztráty záruky a zanedbání údržby IS (upgrade, zejména legislativní upgrade), které mohou vést až k výpadku systému. Tato analýza také podrobně líčí postavení podniku na trhu, jeho slabé a silné

stránky a pomáhá tak k lepšímu pochopení výsledných rizik. Každý podnik je ze zákona povinen každoročně vyplnit požadované účetní výkazy a vytvořit účetní uzávěrku. Účetní uzávěrka přehled veškerých účetních případů za uplynulý rok a dává tak podniku možnost získat užitečné informace, které je možné využít k potřebným ekonomickým analýzám. Výsledky těchto analýz lze dále využít i k určení rizikových faktorů do budoucna.

4.1. Elementární metody finanční analýzy

Princip elementárních metod spočívá na aritmetických operacích s jednotlivými ukazateli. Patří mezi ně tyto metody, viz [7]:

- **Analýza absolutních ukazatelů**
 - Analýza trendů
 - Procentní rozbor
- **Analýza rozdílových ukazatelů**
 - Analýza cash-flow
 - Analýza fondů finančních prostředků
 - Analýza tržeb, nákladů a zisku
- **Analýza poměrových ukazatelů**

Pro účely analýzy finančních rizik vzhledem k IS budeme používat následující ukazatele.

- Ukazatele likvidity

Likvidita je vyjádření schopnosti podniku hradit své krátkodobé závazky.

Likvidita se dělí na tři stupně:

a) L3 – Běžná likvidita

$$L3 = \frac{\textit{Oběžná aktiva}}{\textit{Krátkodobé cizí zdroje}} \quad (4.1)$$

Běžná likvidita vyjadřuje, kolikanásobně dokáže společnost pokrýt své krátkodobé závazky, kdyby všechna svoje oběžná aktiva proměnila na hotovost.

b) L2 – Pohotová likvidita

$$L2 = \frac{\text{Obežná aktiva} - \text{Zásoby}}{\text{Krátkodobé cizí zdroje}} \quad (4.2)$$

Rozdíl mezi běžnou a pohotovou likviditou je v čitateli, kde jsou u pohotové likvidity oběžná aktiva snížena o zásoby.

c) L1 – Okamžitá likvidita

$$L1 = \frac{\text{Krátkodobý finanční majetek}}{\text{Krátkodobé cizí zdroje}} \quad (4.3)$$

Okamžitá likvidita odečítá od oběžných aktiv nejenom zásoby, ale i pohledávky, takže v čitateli zůstane jen krátkodobý finanční majetek, kterým je schopna okamžitě platit.

○ Ukazatele rentability

Rentabilita, neboli také ziskovost firmy, je ukazatel, o kterém můžeme říci, že dává do souvislosti všechny předchozí skupiny s hospodářským výsledkem společnosti.

a) ROI = rentabilita investic

$$ROI = \frac{\text{Zisk před zdaněním}}{\text{Celková aktiva}} \quad (4.4)$$

b) ROA = Výnos na aktiva

$$ROA = \frac{\text{Čistý zisk}}{\text{Celková aktiva}} \quad (4.5)$$

c) ROE = Výnos na vlastní jmění

$$ROE = \frac{\text{Čistý zisk}}{\text{Vlastní kapitál}} \quad (4.6)$$

○ Další ukazatele

a) Spread

$$\text{Spread} = ROE - r_e \quad (4.7)$$

ROE je výnosnost vlastního kapitálu a r_e je alternativní náklad vlastního kapitálu. Spread je ukazatelem úrovně podnikové výkonnosti.

b) Obrat aktiv

$$\text{Obrat aktiv} = \frac{\text{Celkové tržby}}{\text{Celková aktiv}} \quad (4.8)$$

Označuje efektivnost využívání celkových aktiv. Obrat aktiv udává, kolikrát se celková aktiva obrátí za jeden rok, viz [14].

c) Poměr vlastního kapitálu a celkových aktiv

$$\text{Poměr vlastního kapitálu a celkových aktiv} = \frac{\text{Vlastní kapitál}}{\text{Celková aktiva}} \quad (4.9)$$

Pojem, který označuje jaká část podnikových aktiv je financována kapitálem akcionářů, viz [15].

- Testy pro hodnocení stavu podniku, tzv. testy vícerozměrné klasifikace

Tyto testy slouží ke zjištění finanční stability podniku. Většina investorů se snaží zjistit situaci firmy na trhu a zvážit, zda firmě důvěřovat a popřípadě do ní investovat. Ten samý postup využívají bankovní instituce, které se z výsledků snaží odhadnout, zda se vyplatí firmě půjčit prostředky či nikoli.

- **Altmanův test**

| DÍLČÍ VÝPOČTY ALTMANOVA TESTU | |
|------------------------------------|---|
| Ukazatel likvidity | X1 = pracovní kapitál / Celková aktiva |
| Ukazatele rentability aktiv | X2 = Zadržovaný zisk / Celková aktiva |
| | X3 = EBIT ¹ / Celková aktiva |
| Ukazatele zadluženosti | X4 = Tržní hodnota akciového kapitálu / Cizí zdroje |
| Ukazatel řízení aktiv | X5 = Tržby / Celková aktiva |

Tabulka 4.1.a Altmanův test; Zdroj: [8]

Tento test vede k tzv. rovnicím důvěry. Tyto rovnice jsou tři a udávají doporučené výsledné hodnoty, které udávají jakýsi index důvěryhodnosti zdraví firmy.

¹ Zisk před zdaněním a úroky

| | | |
|--------------------------|---|----------------------------|
| 1. Rovnice důvěry | $Z1 = 1,2 X1 + 1,4 X2 + 3,3 X3 + 0,6 X4 + 1,0 X5$ | |
| Doporučené hodnoty: | | |
| Firma je finančně silná | „šedá zóna“ | Firma má finanční problémy |
| $Z1 \in <2,99; 8>$ | $Z1 \in <1,81; 2,98>$ | $Z1 \in <-4; 1,8>$ |

Tabulka 4.1.b První rovnice důvěry; Zdroj [8]

| | | |
|--------------------------|--|----------------------------|
| 2. Rovnice důvěry | $Z2 = 0,717 X1 + 0,847 X2 + 3,107 X3 + 0,42 X4 + 0,998 X5$ | |
| Doporučené hodnoty: | | |
| Firma je finančně silná | „šedá zóna“ | Firma má finanční problémy |
| $Z2 > 2,9$ | $Z2 \in (1,2; 2,9)$ | $Z2 < 1,2$ |

Tabulka 4.1.c Druhá rovnice důvěry; Zdroj: [8]

| | | |
|--------------------------|--|----------------------------|
| 3. Rovnice důvěry | $Z3 = 6,56 X1 + 3,26 X2 + 6,72 X3 + 1,05 X4$ | |
| Doporučené hodnoty: | | |
| Firma je finančně silná | „šedá zóna“ | Firma má finanční problémy |
| $Z3 > 2,6$ | $Z3 \in (1,1; 2,6)$ | $Z3 < 1,1$ |

Tabulka 4.1.d Třetí rovnice důvěry; Zdroj [8]

První rovnice Z1 je pro akciové společnosti, druhá Z2 pro ostatní (neakciové) společnosti a specifická třetí Z3 pro nevýrobní podniky a rozvíjející se trhy.

- **Tafflerův test**

Tento test je jedním z nejpoužívanějších testů k odhalení hrozícího bankrotu firmy.

| |
|--|
| DÍLČÍ VÝPOČTY TAFFLEROVA TESTU |
| $X1 = \text{hrubý zisk} / \text{krátkodobé závazky}$ |
| $X2 = \text{oběžná aktiva} / \text{cizí zdroje}$ |
| $X3 = \text{krátkodobé závazky} / \text{celková aktiva}$ |
| $X4 = \text{tržby} / \text{celková aktiva}$ |

Tabulka 4.1.e Tafflerův test; Zdroj: [9]

Na rozdíl od Altmanova testu využívá Tafflerův model pouze jednu rovnici.

$$\text{Tafflerův bankrotní model} = 0,53X_1 + 0,13X_2 + 0,18X_3 + 0,16X_4$$

Tabulka 4.1.f Tafflerův model; Zdroj: [9]

Jako kritická hodnota neboli mez, pod kterou by firma neměla kvůli hrozícímu bankrotu klesnout, se udává 0,2. Naopak hodnota, nad kterou bankrot firmě nehrozí, je 0,3.

○ **QUICK test (Kralicek)**

Test byl sestaven profesorem Kralickem v roce 1991. Je rozdělen na dvě základní části, což jsou samotný QUICK test a Index bonity. V QUICK testu postupně uděluje známky jednotlivým poměrovým ukazatelům, které se předem vypočtou z dat obsažených ve výročních zprávách, jak je tomu i u dvou předchozích testů. Každý ukazatel pochází z jedné ze čtyř oblastí finanční analýzy, což jsou, viz [10]:

- Finanční část, která znázorňuje míru zadlužení firmy.
- Likvidní část, která udává schopnost firmy včas dostát svým závazkům.
- Rentabilní část, což je ekonomický ukazatel efektivity hospodaření podniku.
- Výnosová část, tedy schopnost firmy uhradit závazky v důsledku fungování.

Následující tabulka blíže přibližuje přehled jednotlivých ukazatelů a funkcionalitu testu.

| Obor analýzy | | Proměnné | Vzorce | Vypovídá o |
|-----------------|--------------------|-------------|---|---------------------|
| Celková situace | Finanční stabilita | Financování | $\frac{\text{Vlastní jmění}}{\text{Bilanční součet}} * 100\%$ | Kapitálové síle |
| | | Likvidita | $\frac{\text{Cizí zdroje} - \text{KFM}^2}{\text{Cash} - \text{flow}}$ | Zadlužení |
| | Výnosová situace | Rentabilita | $\frac{\text{EBIT}^3}{\text{Bilanční součet}} * 100\%$ | Výnosu |
| | | Výnos | $\frac{\text{Cash} - \text{flow}}{\text{Tržby}} * 100\%$ | Finanční výkonnosti |

Tabulka 4.1.g QUICK test; Zdroj: [10]

² Krátkodobý finanční majetek

³ Zisk před zdaněním a úroky

Dále se využívá známkovacího hodnocení, které je uvedeno v další tabulce. Stupnice známky je v rozmezí od 1 do 5, přičemž jednička je velmi dobrý výsledek a pětka je hranice, při které podniku hrozí insolvence.

| Ukazatele | ZNÁMKY | | | | |
|---------------------------------------|--|--------------|----------------------|---------------|---------------------------|
| | Velmi dobrý (1) | Dobrá (2) | Středně dobrá (3) | Špatná (4) | Ohrožen insolvenčí (5) |
| Kvóta vlastního kapitálu | > 30% | > 20% | > 10% | < 10% | < 0% |
| Doba splácení dluhu v letech | < 3 roky | < 5 let | < 12 let | > 12 let | > 30 let |
| Průběžná známka 1: finanční stabilita | Aritmetický průměr hodnocení kvóty vlastního kapitálu a doby splácení Dluhu | | | | |
| Rentabilita celkového kapitálu | > 15% | > 12% | > 8% | < 8% | < 0% |
| Cash-flow v % podnikového výkonu | > 10% | > 8% | > 5% | < 5% | < 0% |
| Průběžná známka 2: výnosová situace | Aritmetický průměr hodnocení rentability celkového kapitálu a Cash-flow v % podnikového výkonu | | | | |
| Celková známka | Aritmetický průměr všech čtyř ukazatelů | | | | |

Tabulka 4.1.h QUICK test; Zdroj: [10]

Pro výpočet indexu bonity, tedy zjištění jestli je firma bonitní, nebo také dobře prosperující se musí spočítat tyto ukazatele, viz [10]:

$$X1 = \frac{\text{Cash} - \text{flow}}{\text{Cizí zdroje}} \quad (4.10)$$

$$X2 = \frac{\text{Bilanční součet}}{\text{Cizí zdroje}} \quad (4.11)$$

$$X3 = \frac{\text{EBT}^4}{\text{Bilanční součet}} \quad (4.12)$$

$$X4 = \frac{\text{EBT}}{\text{Tržby}} \quad (4.13)$$

$$X5 = \frac{\text{Zásoby}}{\text{Tržby}} \quad (4.14)$$

$$X6 = \frac{\text{Tržby}}{\text{Bilanční součet}} \quad (4.15)$$

⁴ Zisk před zdaněním

Z těchto šesti ukazatelů se dále tvoří diskriminační funkce, podle které spočítáme skóre Indexu bonity. Diskriminační funkce vypadá následovně, viz [10]:

$$IB = 1,5X_1 + 0,08X_2 + 10X_3 + 5X_4 + 0,3X_5 + 0,1X_6$$

Tabulka 4.1.i Index bonity; Zdroj: [10]

Výsledky diskriminační funkce se pak hodnotí podle následující tabulky:

| Ohrožen insolencí | | | | Neohrožen insolencí | | | | |
|-------------------|--------------|----------|----------------|---------------------|---------------|------------|-------------|----------------|
| Extrémně špatné | Velmi špatné | Špatné | Středně špatné | Dělicí Hodnota | Středně dobré | Dobré | Velmi dobré | Extrémně dobré |
| -1 a méně | -1 až 0 | 0 až 0,3 | 0,3 až 1 | 1 | 1 až 1,5 | 1,5 až 2,2 | 2,2 až 3 | 3 a více |

Tabulka 4.1.j1 Diskriminační funkce; Zdroj: [10]

5. Analýza rizik informačních systémů vybrané společnosti

Pro analýzu rizik byla vybrána firma GlaxoSmithKline, s. r. o. (dále jen „GSK“), která je v České republice pobočkou jedné z největších farmaceutických firem na světě. Firma se zabývá výzkumem, vývojem, výrobou a prodejem léčivých přípravků a patří mezi přední světové inovátory ve farmaceutickém průmyslu. Toto průmyslové odvětví je v současné době jedním z nejvíce konkurenčních prostředí. Proto ochrana a zabezpečení informačních systémů je pro takovouto firmu zcela zásadní a takový druh podnikání sebou přináší mnohá rizika.

Byla použita kvalitativní metoda analýzy rizik⁵. Pro správné pochopení, jak analyzovat rizika, je nutné detailně vysvětlit fáze vzniku analýzy a popsat jak se získají jednotlivé dokumenty. Tyto fáze jsou v podstatě popsány v teoretické části, takže se výrazy mohou opakovat.

Činnosti, které vedly k vytvoření analýzy rizik, jsou, viz strana 6 této práce:

- Aktiva
 - Identifikace a rozdělení identifikovaných aktiv

⁵ Pro externího pozorovatele firmy je tato metoda více vyhovující, protože pro kvantitativní metodu je zapotřebí více finančních informací ohledně ceny pořízení IS a nákladů na provoz, které nebyly k dispozici

- Ohodnocení rozdělených aktiv
- Hrozby
 - Identifikace
 - Hodnocení hrozeb a jejich dopadů na aktiva
- Rizika
 - Vyhodnocení rizik
 - Vyhodnocení opatření
- Bezpečnostní opatření

5.1. Identifikace aktiv

Mezi aktiva patří vše, co má pro společnost nějakou hodnotu a mělo by být odpovídajícím způsobem chráněno. Z hlediska zaměření této práce ohledně IS jsou zajímavá pouze aktiva s nimi spojená. Byl vytvořen formulář ve spolupráci s pracovníky společnosti GSK, viz Tabulka 5.2.

5.2. Ohodnocení aktiv

Do hodnocení byli zapojeni pracovníci organizace, pro kterou je analýza vykonávána a získat od nich potřebné informace. Tyto číselné hodnoty byly vyplněny do formuláře. Použil jsem tedy následující postup:

1. Vytvoření tabulky pro hodnocení aktiv
2. Vyplnění tabulky

Tabulka s ohodnocenými aktivy vypadá následovně:

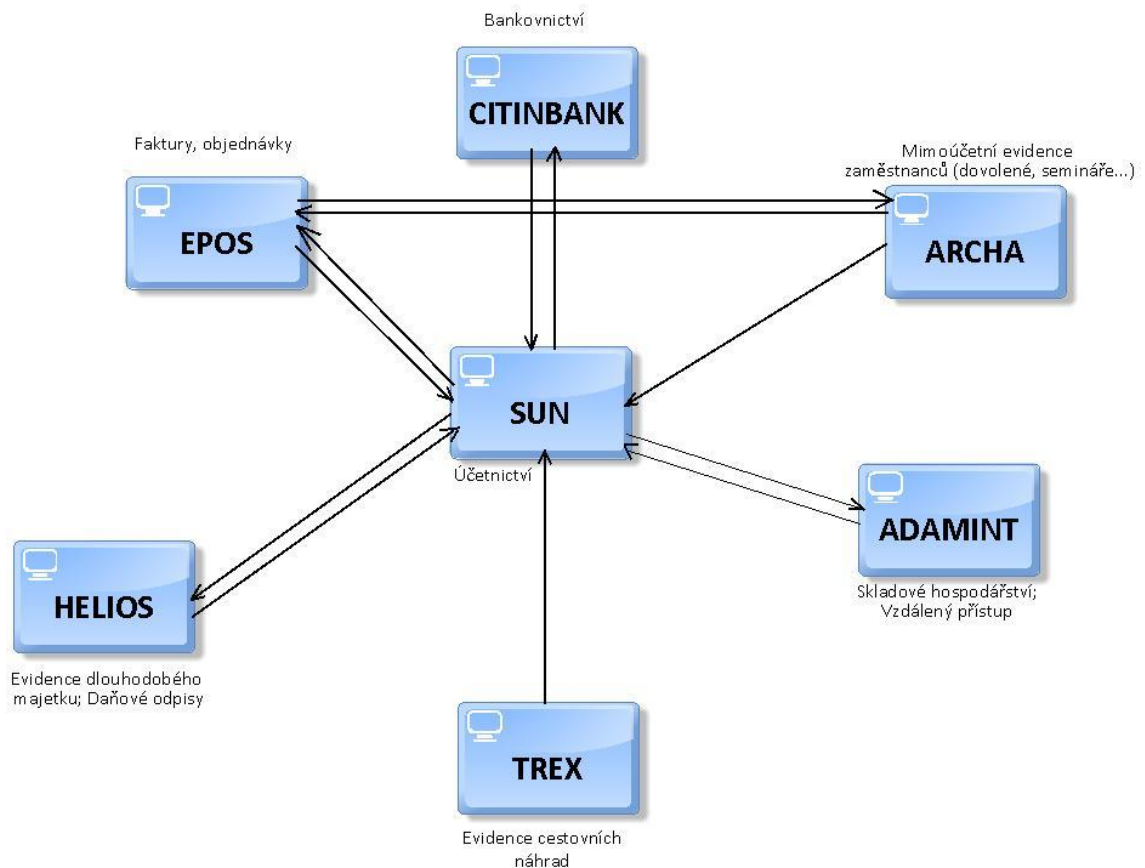
| Identifikované aktivum | Hodnota aktiva v Kč |
|-------------------------------|---------------------|
| Podnikové informační systémy | 14 000 000 |
| Webové stránky | 56 000 |
| Notebooky, tablety, stolní PC | 8 205 000 |
| Ostatní HW | 1 678 120 |
| PC stojany v lékárnách | 2 601 000 |
| Servery | 3 361 000 |
| Telefony, přístroje | 24 239 |
| Budovy | - |
| Lidé ⁶ | - |

Tabulka 5.2. Identifikovaná aktiva k datu: 31.12.2012; Zdroj: firemní dokumentace

5.3. Podnikové informační systémy

Informační systémy jsou nezbytnou součástí chodu podniku takových rozměrů jako je firma GSK. GSK se zabývá jak výrobou, tak i prodejem léčiv, proto ve firmě probíhá velké množství procesů a je potřeba nějak zpracovávat a shromažďovat velké množství dat a informací. Tato skutečnost přivedla firmu k investování do několika informačních systémů různých funkcionalit propojených do podnikového IS. Funkcionalita informačních systémů byla konzultována s pracovníky GSK. IS a propojení jeho komponent včetně informačních toků je na obrázku 5.3. Schéma podnikových IS. Pořizovací ceny jednotlivých IS nebyly pro účely vypracování této práce dostupné.

⁶ Lidé jsou také aktivem firmy, které je třeba zde zmínit, protože se s ním pracuje v další fázi analýzy.



Obrázek 5.3. Schéma podnikových IS a informačních toků mezi jednotlivými subsystémy

5.3.1 SUNsystems

Popis: Účetní software sloužící ke sběru a interpretaci veškerých účetních podnikových dat a informací s možností detailních analýz dle vlastních potřeb.

Funkcionalita systému, viz [17]:

- Finanční účetnictví
- Nákladové účetnictví
- Pohledávky a závazky
- Nákup a prodej
- Pokladna
- Majetek
- Finanční plánování, finanční analýza

Rok pořízení: 2002

Výrobce: Infor, <http://www.infor.com/>

5.3.2 CITIBANK

Popis: Bankovní systém pro interakci s bankou Citibank.

Funkcionalita systému, viz [20]:

- Sledování pohybů a zůstatků na všech účtech včetně cizoměnových účtů a účtů vedených v zahraničních pobočkách Citi nebo třetích bank
- Zobrazení a tisk elektronických výpisů do PDF, XLS a DOC formátů
- Zasílání výpisu a reportu do emailové schránky v předem nastaveném čase
- Vytváření a odesílání zahraničních, tuzemských platebních příkazů a inkas
- Odesílání korunových expresních plateb
- Zasílání zabezpečených elektronických zpráv
- Import a export dat pro komunikaci s účetním systémem
- Nastavení až devíti stupňové autorizace platebních instrukcí

Rok pořízení: 2002

Výrobce: Citi, <http://www.citi.com/czech/home/index.htm>

5.3.3 EPOS

Popis: Jedná se o elektronický objednávkový systém. Tato aplikace umožňuje přehlednou evidenci faktur a tvorbu objednávek pro nákupy režijních služeb a zboží včetně analýz nákupů a dalšího reportingu. V podstatě funguje jako databáze dodavatelů, ale i odběratelů, která obsahuje veškeré potřebné informace, jako jsou kontakty, smlouvy, objednávky a následné faktury, procesy a další aktivity dodavatelů spojené se společností. Do EPOSu mohou zadávat data pouze asistentky na základě aktivit, které předem dohodli manažeři firmy. Bez tohoto systému nemohou probíhat objednávky přijímané od zákazníků a ani objednávky odeslané k dodavatelům.

Funkcionalita systému, viz [18]:

- Objednávky
- Zakázky
- Rozpočty/kalkulace
- Faktury/doklady
- Výkony/Náklady
- Dokumenty
- Ceníky
- Rok pořízení: 2002
- Výrobce: EPOS PRO, s.r.o. <http://www.epos.cz/>

5.3.4 TREX

Popis: Internetová aplikace, která umožňuje snadné a rychlé zpracování cestovních náhrad. Na jedné straně s ním zacházejí sami zaměstnanci a vypisují do něj uplynulé události a na druhé straně jsou tyto data zpracovávána finančním oddělením. Systém obsahuje veškeré informace o cestovních záležitostech, jako jsou přesné datum cest, výdaje na cestách, nebo lokality, kam zaměstnanci GSK putují. Systém je přímo napojen na zaměstnanecké kreditní karty, které slouží výhradně k placení výdajů za cestování. Jakmile zaměstnanec použije kreditní kartu k placení, systém TREX tuto událost zaznamená a shromáždí informace.

Funkcionalita systému, viz [19]:

- evidence vozidel a jejich držitelů
- vedení knihy jízd
- vykazování výdajů z domácích i zahraničních cest
- tvorba a schvalování cestovních příkazů, jejich vyúčtování
- evidence vyplacených hotovostních záloh, sledování výběrů z bankomatů, výměny peněz
- podpora více měn, diet v různých státech
- uživatelská definice typů dokladů a pravidel pro jejich vyplnění
- kontrola výpisu platebních karet

Rok pořízení: 2005

Výrobce: COMPAREX CZ s.r.o., <http://www.comparex-group.com/web/cz/cz/main.htm>

5.3.5 HELIOS

Popis: Pomocná aplikace využívaná pro evidenci dlouhodobého majetku. Pomáhá evidovat údaje pro daňové účely.

Funkcionalita systému, viz [21]:

- Evidenční karta majetku - evidenční formulář obsahující informace o majetku, ze kterého lze současně provádět jednopoložkové i dávkové změnové operace nad položkami majetku a spouštět další související funkce uvedené níže
- Základní změnové operace - zařazení, oprava, převod, doučtování a vyřazení
- Evidence inventurních rozdílů
- Evidence přírůstků
- Uživatelské vztahy - údaje o výpůjčkách, pronájmech, věcných břemenech, zástavních smlouvách a podobných vztazích vázaných k položce majetku
- Odkazy - možnost uložení a otevírání odkazů na externí soubory nebo internetové adresy
- Přenos dat do účetnictví
- Úprava a vyrovnání odpočtu DPH
- Odpisy - evidence majetku umožňuje zpracování daňových a účetních odpisů položek dlouhodobého majetku movitého a budov

Rok pořízení: 2006

Výrobce: Asseco Solutions, a.s., <http://www.helios.eu/cz.html>

5.3.6 ARCHA

Popis: Tato na zakázku vytvořená aplikace slouží pro potřeby podrobné evidence aktivit zaměstnanců firmy a schvalování událostí pořádaných firmou. Zadávají se sem časy pořádaných seminářů, kontakty na zřizovatele podnájmů pro konání akcí. Funguje jako archiv a mají do něj přístup všichni zaměstnanci. Dále také umožňuje zaměstnancům žádat o dovolenou a řídí zprávy z jejich datových schránek. Archiv obsahuje také

veškeré informace o zaměstnancích, jako telefonní čísla, datové schránky zpráv, dokumentace, datum konání akcí, které má právě zkoumaný zaměstnanec na starosti, rozpočet přidělený pro tuto akci. Je propojený se systémem EPOS - pokud například proběhne nějaká objednávka a zaznamená se do EPOSu, tak se došlá fakturace okamžitě stane přístupnou v systému ARCHA.

Rok pořízení: 2009

Výrobce: EPOS PRO, s.r.o., <http://www.epos.cz/>

5.4. Realizace finanční analýzy

Finanční analýza byla vypracována jako obecná aplikace finanční analýzy v programu Microsoft Excel podle jednotlivých ukazatelů rozebraných v teoretické části práce. Výsledné hodnoty ukazatelů jsem porovnal s benchmarkingovým diagnostickým systémem finančních indikátorů INFA, dostupným na webu Ministerstva průmyslu a obchodu ČR, viz [16]. Tento systém ukazuje průměrné hodnoty ukazatelů zkoumaného odvětví pro jednotlivá účetní období, se kterými se výsledné hodnoty společnosti GSK porovnávají. Nyní výsledky pouze shrnu a vyvodím závěry. Pro definování postavení firmy a její finanční stability jsem nepoužil všechny ukazatele uvedené v teoretické části, ale pouze ty z nich, které jsou nejlépe vypovídající. Kompletní finanční analýza je pak dostupná jako příloha této práce na CD. Pro účely hodnocení benchmarkingovým systémem jsem zařadil společnost GSK podle CZ-NACE do odvětví č.21 – Výroba farmaceutických výrobků.

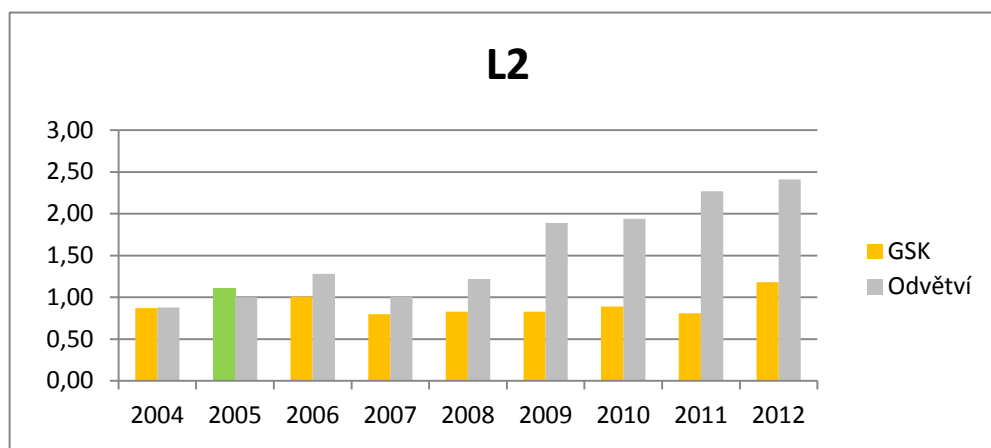
5.4.1 Výsledky:

A. Likvidita

a. Pohotovú likvidita (L2)

| L2 | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 |
|---------|------|------|------|------|------|------|------|------|------|
| GSK | 0,87 | 1,11 | 1,01 | 0,80 | 0,83 | 0,83 | 0,89 | 0,81 | 1,18 |
| Odvětví | 0,88 | 1,00 | 1,28 | 1,01 | 1,22 | 1,89 | 1,94 | 2,27 | 2,41 |

Tabulka 5.4.a Pohotovú likvidita



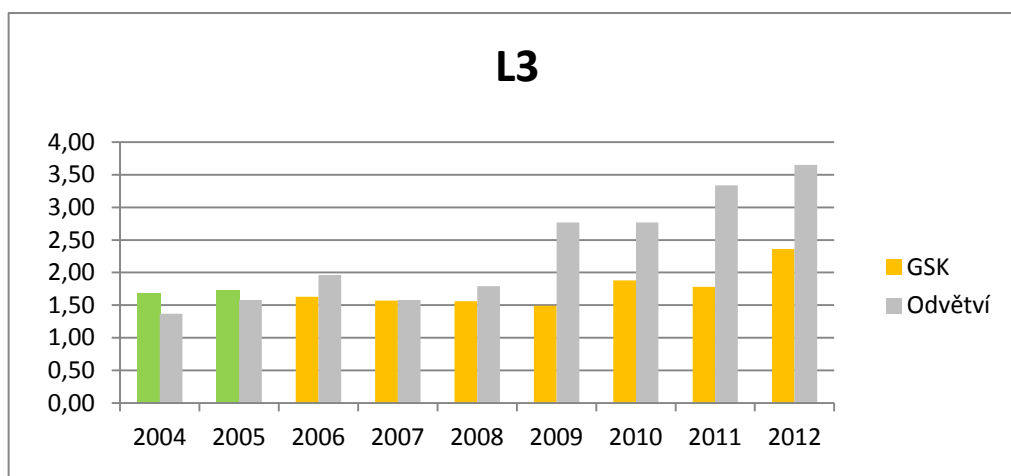
Graf 5.4.a Pohotovú likvidita

Hodnoty jsou kromě roku 2005 mírně horší než hodnoty odvětví, avšak jsou to celkově dobré hodnoty, s odvětvím takřka srovnatelné.

b. Běžná likvidita (L3)

| L3 | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 |
|---------|------|------|------|------|------|------|------|------|------|
| GSK | 1,68 | 1,73 | 1,63 | 1,57 | 1,56 | 1,49 | 1,88 | 1,78 | 2,36 |
| Odvětví | 1,37 | 1,58 | 1,96 | 1,58 | 1,79 | 2,77 | 2,77 | 3,34 | 3,65 |

Tabulka 5.4.b Běžná likvidita



Graf 5.4.b Běžná likvidita

Také hodnoty běžné likvidity vyšly srovnatelně s odvětvím ve všech letech.

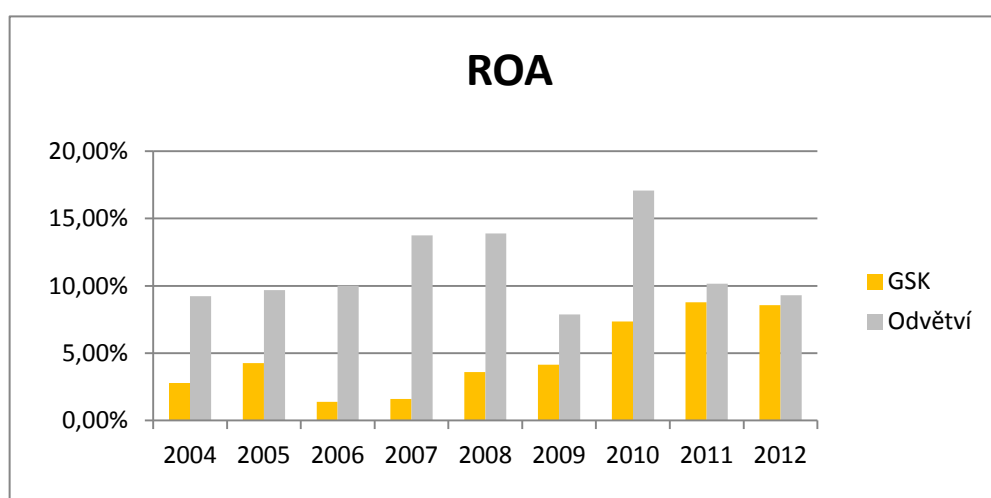
Z dobrých hodnot můžeme usuzovat, že likvidita firmy, tedy schopnost firmy získat prostředky pro úhradu svých závazků je dostačující a firma se z tohoto pohledu jeví jako finančně silná.

B. Rentabilita

a. ROA – produkční síla

| ROA | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 |
|---------|-------|-------|--------|--------|--------|-------|--------|--------|-------|
| GSK | 2,79% | 4,25% | 1,39% | 1,61% | 3,59% | 4,14% | 7,36% | 8,77% | 8,57% |
| Odvětví | 9,22% | 9,69% | 10,02% | 13,75% | 13,88% | 7,87% | 17,08% | 10,16% | 9,30% |

Tabulka 5.4.c2 Produkční síla



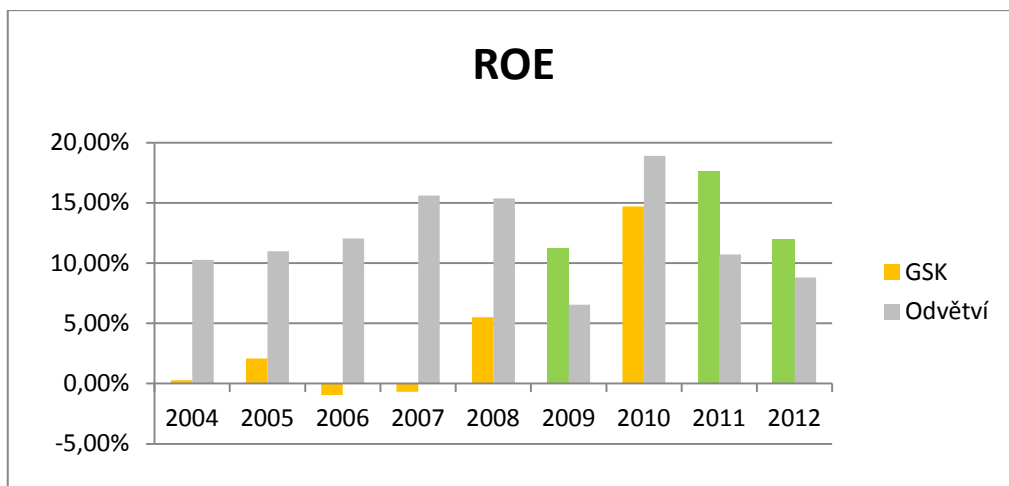
Graf 5.4.c Produkční síla

Poněkud nízké hodnoty se postupem let zvyšují a srovnávají se s odvětvím.

b. ROE - rentabilita vlastního kapitálu

| ROE | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 |
|---------|--------|--------|--------|--------|--------|--------|--------|--------|--------|
| GSK | 0,28% | 2,08% | -0,95% | -0,68% | 5,52% | 11,20% | 14,70% | 17,61% | 11,97% |
| Odvětví | 10,28% | 11,00% | 12,04% | 15,62% | 15,38% | 6,55% | 18,92% | 10,73% | 8,80% |

Tabulka 5.4.d Rentabilita vlastního kapitálu



Graf 5.4.d Rentabilita vlastního kapitálu

Hodnoty se postupem času opět zvyšují a v posledních dvou letech dokonce převyšují hodnoty odvětví.

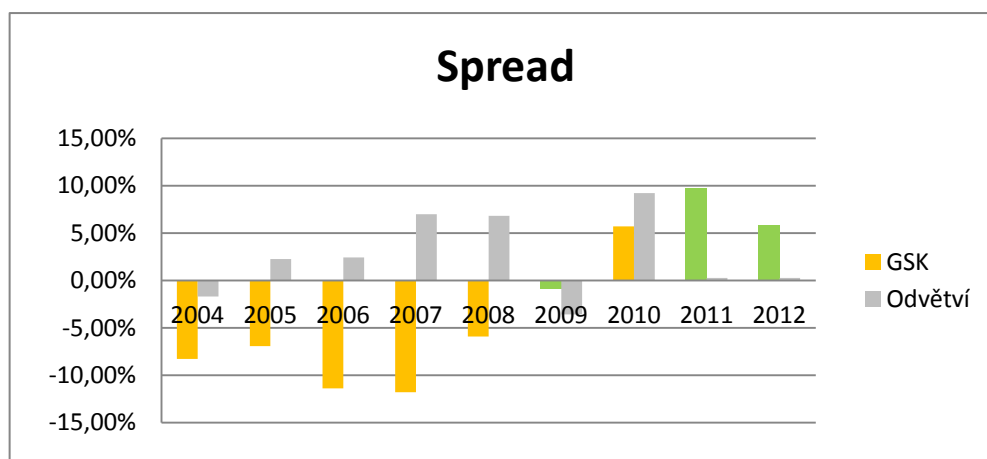
Jelikož je rentabilita podniku ukazatel výnosnosti, nebo lépe řečeno schopnost firmy dosahovat výnosu, lze z těchto hodnot vyvodit fakt, že firma je dobře prosperující.

C. Další ukazatele

a. Spread

| Spread | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 |
|---------|--------|--------|---------|---------|--------|--------|-------|-------|-------|
| GSK | -8,26% | -6,92% | -11,38% | -11,78% | -5,92% | -0,83% | 5,71% | 9,75% | 5,81% |
| Odvětví | -1,70% | 2,25% | 2,42% | 6,99% | 6,83% | -3,58% | 9,23% | 0,26% | 0,27% |

Tabulka 5.4.e3 Spread



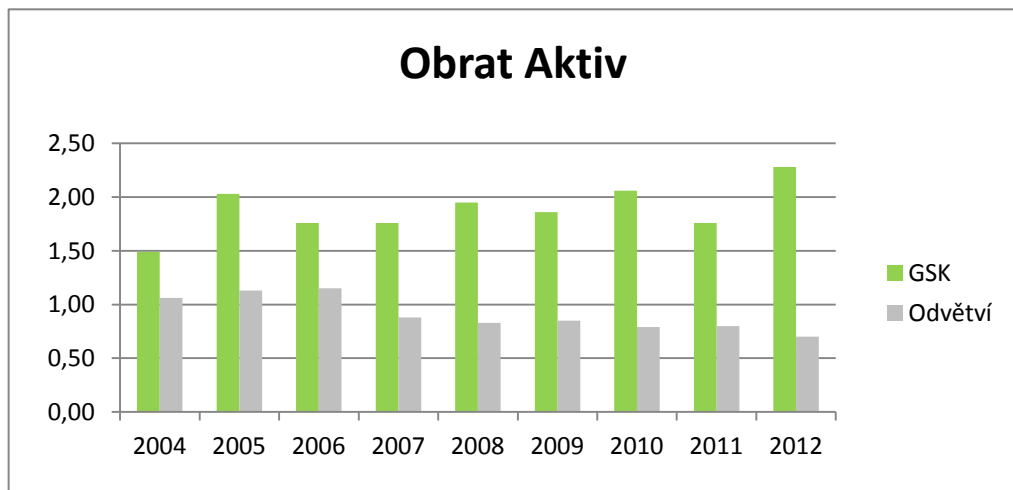
Graf 5.4.e Spread

I u ukazatele Spread je zřejmá tendence růstu v průběhu let. V posledních třech letech jsou hodnoty velmi dobré.

b. Obrat aktiv

| Obrat Aktiv | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 |
|-------------|------|------|------|------|------|------|------|------|------|
| GSK | 1,49 | 2,03 | 1,76 | 1,76 | 1,95 | 1,86 | 2,06 | 1,76 | 2,28 |
| Odvětví | 1,06 | 1,13 | 1,15 | 0,88 | 0,83 | 0,85 | 0,79 | 0,80 | 0,70 |

Tabulka 5.4.f Obrat aktiv



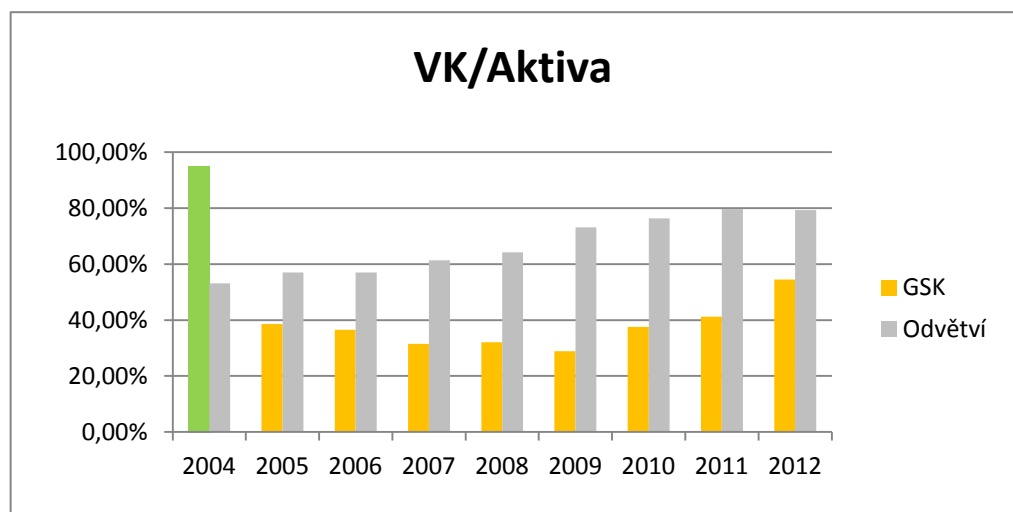
Graf 5.4.f Obrat aktiv

Obrat aktiv ve všech letech převyšuje hodnoty odvětví, což je velmi dobrý výsledek.

c. Poměr vlastního kapitálu a celkových aktiv

| VK/aktiva | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 |
|-----------|--------|--------|--------|--------|--------|--------|--------|--------|--------|
| GSK | 95,04% | 38,57% | 36,54% | 31,51% | 32,07% | 28,81% | 37,53% | 41,26% | 54,49% |
| Odvětví | 53,14% | 57,02% | 56,97% | 61,38% | 64,24% | 73,08% | 76,33% | 79,70% | 79,32% |

Tabulka 5.4.g Poměr vlastního kapitálu a celkových aktiv



Graf 5.4.g Poměr vlastního kapitálu a celkových aktiv

Také tento ukazatel se po většinu let drží na dobrých hodnotách v porovnání s odvětvím.

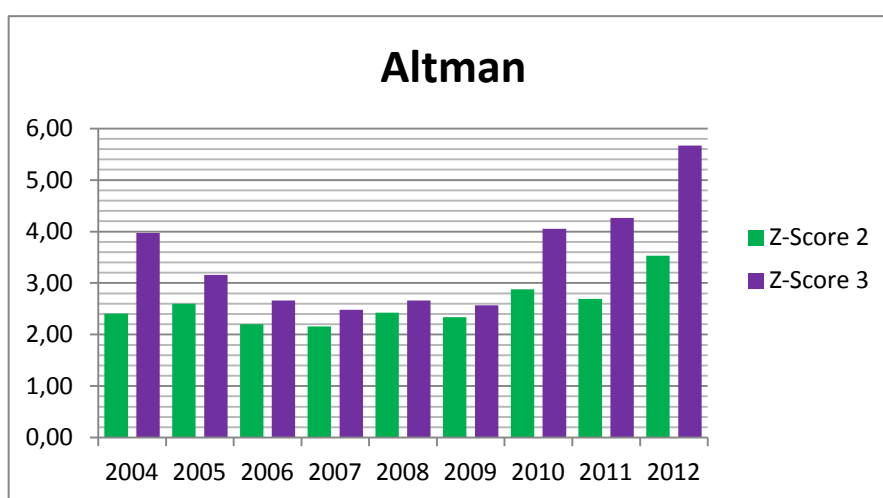
D. Testy vícerozměrné klasifikace

a. Altmanův test

GSK je společnost s.r.o., proto jsem použil pouze dva odpovídající ukazatele Altmanova testu, tedy Z-score 2 pro neakciové společnosti a Z-Score 3 pro ostatní nevýrobní podniky, protože za takovou firmu se dá tato firma vzhledem k veškerým aktivitám také považovat.

| Altmanův test | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 |
|---------------|------|------|------|------|------|------|------|------|------|
| Z-Score 2 | 2,40 | 2,60 | 2,20 | 2,16 | 2,42 | 2,34 | 2,88 | 2,69 | 3,53 |
| Z-Score 3 | 3,97 | 3,16 | 2,66 | 2,48 | 2,66 | 2,56 | 4,05 | 4,26 | 5,67 |

Tabulka 5.4.h Výsledky Altmanova testu



Graf 5.4.h Výsledky Altmanova testu

Z-Score 2 – Hranice, pod kterou by neměly hodnoty vyjít, aby se dalo hovořit o nedostatečných výsledcích a tím pádem neprosperujícím podniku je hodnota 2,9. Ve většině let je tato hranice těsně na dosah a v posledním zkoumaném roce 2012 ji dokonce převyšuje.

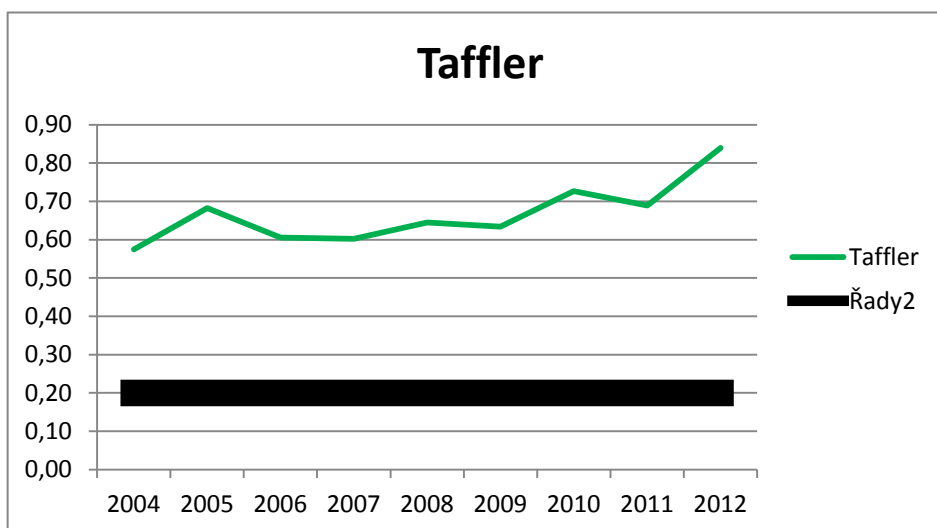
Z-Score 3 – Zde by se hodnoty měly podle Altmana pohybovat nad hranicí 2,6. Ve všech letech je tato hranice překonána s výjimkami v letech 2007 a 2009.

Výsledné hodnoty hovoří o GSK jako o finančně silném podniku.

b. Tafflerův test

| Tafflerův test | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 |
|----------------|------|------|------|------|------|------|------|------|------|
| TAFFLER | 0,57 | 0,68 | 0,61 | 0,60 | 0,65 | 0,63 | 0,73 | 0,69 | 0,84 |

Tabulka 5.4.i Výsledky Tafflerova testu



Graf 5.4.i Tafflerův bankrotní model

Tento test zjišťuje bankrotní míru rizika. Podnik, jehož hodnoty jsou nad hranicí 0,3, je od bankrotu velmi vzdálen, proto i tento test ukazuje, že firma je finančně stabilní.

c. QUICK test

| QUICK test [Kralicek] | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 |
|-----------------------|------|------|------|------|------|------|------|------|------|
| celková známka | 3,8 | 3,0 | 3,3 | 3,3 | 3,0 | 3,3 | 2,5 | 2,8 | 2,5 |

Tabulka 5.4.j Výsledky QUICK testu

Podle Kralicka by se měl podnik pohybovat pod hranicí 3,0. Z tohoto pohledu se tyto hodnoty mohou jevit jako horší, může to však plynout z nastavení známkování pro Rakousko v 90. letech minulého století, kdy byl test konstruován.

| Index bonity [Kralicek] | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 |
|-------------------------|------|------|------|------|------|------|------|------|------|
| IB Kralicek | 0,56 | 1,07 | 0,58 | 0,62 | 0,90 | 1,01 | 1,64 | 1,67 | 1,82 |

Tabulka 5.4.k Index bonity

Z počátku hodnoty bonity nejsou nijak vysoké, ale postupem let se podnik dostává do stále lepších, bonitních hodnot.

E. Závěr

| Výsledky jednotlivých testů ⁷ | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 |
|--|------|------|------|------|------|------|------|------|------|
| Z2 | ? | ? | ? | ? | ? | ? | ? | ? | + |
| Z3 | + | + | + | ? | + | ? | + | + | + |
| Taffler | + | + | + | + | + | + | + | + | + |
| QUICK-test | - | - | - | - | - | - | ? | ? | ? |
| IB | + | + | + | + | + | + | + | + | + |

Tabulka 5.4.l Výsledky testů vícerozměrné klasifikace

Zde jsou shrnuty výsledky jednotlivých testů, symboly jsou vysvětleny v poznámce pod čarou.

| Benchmarking ⁸ | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 |
|---------------------------|------|------|------|------|------|------|------|------|------|
| L2 | ? | + | - | - | - | - | - | - | - |
| L3 | + | + | ? | ? | ? | - | - | - | - |
| ROA | - | + | - | - | - | - | - | ? | ? |
| ROE | - | - | - | - | - | + | - | + | + |
| Spread | - | - | - | - | - | + | - | + | + |
| Obrat aktiv | + | + | + | + | + | + | + | + | + |
| VK/Aktiva | + | - | - | - | - | - | - | - | - |

Tabulka 5.4.m Výsledky Benchmarking

V této tabulce jsou shrnuty výsledky benchmarkingu.

Všechny tyto ukazatele dohromady prokázaly, že firma GSK je dobře prosperujícím podnikem, kterému se v průběhu let daří. I když je společnost v některých parametrech pod oborovým průměrem, v základních ukazatelích se jeví jako stabilní. Finanční rizika mu tedy téměř nehrozí, pokud se bude finančně vyvíjet jako doposud.

5.5. Riziko investice do informačních systémů

Po zhodnocení finanční prosperity firmy zhodnotím i riziko spojené s nákupem jednotlivých informačních systémů, lépe řečeno zkoumám fakt, jestli je firma schopna tuto investici pokrýt, aniž by se dostala do finančních problémů. U poslední dostupné účetní uzávěrky z roku 2012 zjišťujeme, že podnikové informační systémy mají zůstatkovou hodnotu 14mil.Kč k 31.12.2012. Tato hodnota byla potvrzena i vedením

⁷ „+“ podle daného testu prosperuje
 „-“ podle daného testu neprospereje
 „?“ šedá zóna (nedokážeme jednoznačně určit)

⁸ „+“ lepší než odvětví
 „-“ slabší než odvětví
 „?“ srovnatelný s odvětvím

firmy a bylo potvrzeno, že jde opravdu o celkovou zůstatkovou hodnotu softwarových systémů popsaných již dříve v práci (viz. kapitola 8.3.). Protože jsem neměl k dispozici úplnou pořizovací cenu IS jako celku, budu dále pracovat v analýze rizik s touto zůstatkovou hodnotou. Nyní tuto hodnotu procentuálně porovnám s důležitými finančními atributy k roku 2012, aby bylo zřejmé jak velké procento a tedy i riziko tato investice tvoří. Pro představu poslouží následující tabulka:

| Finanční atribut firmy | Hodnota atributu v Kč | Zůstatková hodnota investice v Kč k 31.12.2012 | % porovnání |
|-----------------------------|-----------------------|--|--------------|
| Celková aktiva | 2511514000,00 | 14000000,00 | 0,56% |
| Hospodářský výsledek | 163809000,00 | 14000000,00 | 8,55% |
| Základní jmění | 1102308000,00 | 14000000,00 | 1,27% |
| Vlastní jmění | 1368504000,00 | 14000000,00 | 1,02% |
| Celkové náklady | 2879143000,00 | 14000000,00 | 0,48% |
| Celkové výnosy | 3180965000,00 | 14000000,00 | 0,44% |

Tabulka 5.5.4 Hodnota investice - hodnoty f. atributů jsou k 31.12.2012

Tato tabulka znázorňuje, kolik procent z jednotlivých finančních atributů tvoří investice do informačních systémů. Z výsledků je patrné, že ve většině případů netvoří investice ani jediné procento z daného atributu. Spolu s faktem, že firma byla po provedení finanční analýzy shledána jako dobře prosperující, lze tedy vyvodit závěr, že riziko financování IS je zanedbatelné. Naopak tato investice pomůže zefektivnit veškeré činnosti vedoucí k lepší prosperitě. Firma má dostatek prostředků na investice tohoto typu a nemusí se obávat případných rizikových faktorů.

5.6. Riziko výpadku informačního systému

Riziko spojené s výpadkem některého ze systémů spočívá vlastně v ohrožení potencionálních zisků firmy. Některé ze systémů přímo spolupracují se zákazníky a dodavateli. Systém EPOS slouží jako objednávkový systém (viz. 8.3.3.) což znamená, že komunikace s dodavateli probíhá přímo přes něj a zadávají se do něj dokumenty online přímo v čase uskutečnění nějaké objednávky. Pokud tedy výpadek takového systému bude mít trvání delší než jeden den, lze předpokládat určité finanční ztráty z výpadku obchodní činnosti. Pokusím se nyní takové riziko vyčíslit.

Pro ohodnocení finanční ztráty budeme uvažovat 100% výpadek obchodní činnosti, tedy nejhorší možnou variantu. Vycházet budeme z průměrné denní tržby. Použil jsem

hodnoty z výroční zprávy z roku 2012, která se nejvíce blíží současné realitě. Jako první vyčísím celkové tržby za rok 2012 z prodeje zboží, výrobků a služeb, viz vzorec (5.6.1):

$$\text{Tržby} = (\text{Tržby za prodej zboží} + \text{Výkony celkem}) \quad (5.6.1)$$

$$\text{Tržby} = (3\,693\,025\,000 + 2\,042\,257\,000) = 5\,735\,282\,000\text{Kč}$$

Pro průměrnou denní tržbu pak platí:

$$\text{Průměrná denní tržba} = \frac{5\,735\,282\,000}{365} \doteq 15\,713\,101\text{Kč}$$

Variantně lze provést výpočet, který bude vycházet jen z tržeb za prodej zboží. Pak průměrná denní tržba je:

$$\text{Tržby za prodej zboží} = 3\,693\,025\,000$$

$$\text{Průměrná denní tržba} = \frac{3\,693\,025\,000}{365} \doteq 10\,117\,876\text{Kč} \quad (5.6.2)$$

Po přezkoumání těchto výsledků lze tedy mluvit o denních ztrátách, které mohou dosáhnout až řádů milionů Kč (od 10 mil. Do 15 mil.). V případě výpadku systému EPOS nemohou probíhat objednávky a v krajním případě hrozí i riziko ztráty zákazníka. Zákazník totiž raději zvolí dostupnou konkurenci, která je na farmaceutickém trhu obrovská.

5.7. Ohodnocení případných škod dopadu na aktiva

Nyní aktiva firmy ohodnotím podle toho, jak jsou pro přežití podniku důležitá. Mezi finančními náklady a tímto pohledem je totiž velký rozdíl. Některé prvky informačního systému nemusí být finančně nejnáročnější, avšak pro přežití podniku, nebo pro jeho standardní chod, jsou klíčové. Toto ohodnocení je důležité pro další práci na analýze rizik. Jako měřicí prvek navrhnu jakousi škálu dopadu, kterou logicky vytvořím při pohledu na jednotlivá aktiva, podle toho jak velké škody mohou na aktivech způsobit. Škálu rozdělím na tři oddělená pásma, a jednotlivá aktiva budou do těchto pásem zapadat, podle toho jak jsou pro podnik důležitá.

Postup je tedy následující:

1. Vytvořit tři pásma a definovat hodnoty škály
2. Zařadit aktiva do jednotlivých pásem

| Pásma | Míra dopadu | Škála (od – do) |
|-------|---------------------------------------|-----------------|
| 1 | Zanedbatelné škody | (0-3) |
| 2 | Vážné škody | (4-6) |
| 3 | Škody ohrožující přežití/chod podniku | (7-9) |

Tabulka 5.7. Škála dopadu na aktiva

Pokud jsou tedy ohrožena aktiva z prvního pásma, mohou být velmi snadno a rychle nahrazena jinými a podnik neutrpí v podstatě žádnou újmu (například fyzické poškození nějakého hardwaru). Aktiva z druhého pásma už nejsou zanedbatelná a jejich ztráta nebo nečinnost může podniku přinést finanční ztráty (například selhání některých softwarových aplikací, může na čas zbrzdit komunikaci s dodavateli a odběrateli). Aktiva ze třetího pásma jsou pro podnik klíčová a jejich ohrožení je pro podnik kritické, neznamená však vždy přímé ohrožení podniku (například výpadek, či dokonce ztráta databáze vyvíjených léčiv a hodnoty s tímto spojené).

5.8. Zařazení aktiv do pásem

Tato tabulka byla vytvořena ve spolupráci s pracovníky firmy GSK.

| Identifikované aktivum | Hodnota - Škála | Pásma |
|---------------------------------------|-----------------|-------|
| Podnikové informační systémy | 7 | 3 |
| Webové stránky | 5 | 2 |
| Notebooky, tablety, stolní PC | 2 | 1 |
| Tiskárny, klávesnice, myši a další HW | 1 | 1 |
| PC stojany v lékárnách | 2 | 1 |
| Servery | 9 | 3 |
| Telefony, přístroje | 4 | 2 |
| Budovy | 6 | 2 |
| Lidé | 9 | 3 |

Tabulka 5.8. Zařazení aktiv do pásem

Nyní je seznam ohodnocených aktiv kompletní a znám jejich význam pro podnik, mohu tak přejít k hrozbám.

6. Hrozby

6.1. Identifikace hrozeb

Nyní určím veškeré hrozby, které mohou na informační systém podniku působit. Hrozby jsou faktory, činnosti a jevy, které mohou určitým způsobem ohrožovat jednotlivá aktiva a působit tak na nich finanční ztráty podniku nebo je dokonce úplně zničit. Hrozby na aktiva působí nepřetržitě a úkolem podniku je těmto hrozbám předcházet. Jak jim předcházet budu řešit na konci analýzy, kdy určím bezpečnostní opatření pro zkoumanou společnost.

Opět jsem tedy použil tabulku aktiv a snažil jsem se určovat a sledovat jevy, které by je mohly ohrozit. Jednotlivé typy hrozeb jsem nastudoval z nejrůznějších zdrojů a použil jsem ty, které se nejvíce vyskytují v prostředí informačních technologií. Nakonec jsem je rozdělil na dvě základní skupiny, podle původu jejich vzniku. Takto vznikla skupina hrozeb způsobených prostředím a skupina hrozeb způsobených lidmi. Na tomto základě jsem vyprodukoval nový seznam hrozeb, který vypadá následovně:

- Hrozby prostředí
 - Požár
 - Výpadek elektrického proudu
 - Selhání hardwaru
 - Selhání softwaru
 - Selhání sítě
- Hrozby způsobené lidmi
 - Chyba správce
 - Chyba uživatele
 - Kyberterorismus
 - Odposlouchávání
 - Použití škodlivého softwaru

Tento seznam jsem předal pracovníkům firmy, se kterými jsem spolupracoval, aby potvrdili, že podobné jevy opravdu mohou nastat a případně ohrozit podnik.

6.1.1 Rozdělení hrozeb podle možnosti vzniku

Nyní hrozby rozdělím podle jejich možného vzniku. Z nastudovaných zdrojů jsem došel k závěru, že hrozby působící na aktiva se dále dělí podle skutečnosti, v jakém smyslu na dané aktivum působí a jakým způsobem je ohrožuje. V zásadě může být na aktivu ohrožena jeho:

1. Důvěrnost
2. Integrita
3. Dostupnost

Dále je důležité vědět, jak daná hrozba vznikne. Opět existují tři faktory, a to tyto:

1. Náhoda
2. Úmysl
3. Přírodní faktor

V závěru je tedy nutno dodat, že jsem hrozby sledoval ze dvou pohledů:

1. Z pohledu bezpečnostních atributů, na které hrozby působí. Tedy důvěrnost, integrita a dostupnost a původ jejich vzniku, jež může být náhoda, úmysl a přírodní faktor.
2. Z pohledu působení hrozeb na skupiny aktiv.

6.1.2 Vyplnění tabulek

Po předložení seznamu a další diskuzi s respondenty jsem vytvořil další dvě tabulky hrozeb a vyplnil je (viz. Tab. 6.1.a a 6.1.b)

| Hrozba | Bezpečnostní atribut | | | Původce vzniku | | |
|-----------------------|----------------------|-----------|------------|----------------|-------|----------|
| | Důvěrnost | Integrita | Dostupnost | Náhoda | Úmysl | Přírodní |
| Požár | | x | x | x | x | x |
| Výpadek el.proudu | | x | x | x | | x |
| Chyba správce | x | x | x | x | x | |
| Chyba uživatele | x | x | x | x | x | |
| Kyberterorismus | x | x | x | | x | |
| Odposlouchávání | x | | | | x | |
| Použití škodlivého SW | x | x | x | x | x | |
| Selhání HW | x | x | x | x | | x |
| Selhání SW | x | x | x | x | | x |
| Selhání sítě | | x | x | x | | x |

Tabulka 6.1.a Původ hrozeb

Jeden z důvodů, proč jsem vytvářel seznam aktiv a rozděloval je na různé skupiny, je právě tento krok. Nyní určím hrozby, které na skupiny aktiv působí.

| Hrozba | Hardware | Software | Sít | Média | Data | Personál | Prostory |
|-----------------------|----------|----------|-----|-------|------|----------|----------|
| Požár | x | | x | x | | x | x |
| Výpadek el.proudu | x | | x | | x | | x |
| Chyba správce | x | x | x | x | x | | |
| Chyba uživatele | x | x | x | x | x | | |
| Kyberterorismus | | x | x | | | | |
| Odposlouchávání | | | x | | | | |
| Použití škodlivého SW | | x | x | | x | | |
| Selhání HW | x | | | | | | |
| Selhání SW | | x | | | | | |
| Selhání sítě | | | x | | | | |

Tabulka 6.1.b Působení hrozeb na skupiny aktiv

Právě teď mám ucelený pojem o hrozbách působících na aktiva firmy. Mohu tedy přejít k dalšímu kroku, což je hodnocení hrozeb.

6.2. Hodnocení hrozeb

Pro stanovení úrovně jsem opět hrozby rozdělil do škály podle pravděpodobnosti jejich naplnění. Stejně jako u hodnocení aktiv jsem použil tři pásma. Hrozby jsem hodnotil v intervalu 0 až 9, přičemž 0 znamená, že naplnění hrozby je nepravděpodobné a 9 naopak, že naplnění hrozby je velmi pravděpodobné. Například rozdíl mezi

pravděpodobností poničení budovy, či hardwaru zemětřesením a chybou, kterou udělá správce je jistě veliký.

Postup byl tedy následující:

1. Vytvořit tři pásma a definovat hodnoty škály
2. Zařadit hrozby do jednotlivých pásem

| Pásma | Hrozba | Škála (od – do) |
|-------|---------------------|-----------------|
| 1 | Nepravděpodobná | (0-3) |
| 2 | Více pravděpodobná | (4-6) |
| 3 | Velmi pravděpodobná | (7-9) |

Tabulka 6.2.a Škála hrozeb; Zdroj:[4]

Tuto škálu nyní použijí na ohodnocení jednotlivých hrozeb podle pravděpodobnosti napadení aktiv.

| Identifikované hrozby | Hodnota – škála | Pásma |
|-----------------------|-----------------|-------|
| Požár | 2 | 1 |
| Výpadek el.proudu | 4 | 2 |
| Chyba správce | 7 | 3 |
| Chyba uživatele | 5 | 2 |
| Kyberterorismus | 4 | 2 |
| Odposlouchávání | 4 | 2 |
| Použití škodlivého SW | 5 | 2 |
| Selhání HW | 9 | 3 |
| Selhání SW | 9 | 3 |
| Selhání sítě | 7 | 3 |

Tabulka 6.2.b Hrozby zařazené do pásem

Nyní jsou vyhodnocená aktiva i hrozby. Aktiva jsou majetkem, který si daná firma snaží chránit, a hrozby jsou škodlivé vlivy, které na ně působí. Dohromady se tyto dvě třídy spojují v rizika. Pro další práci mám tedy dostatek informací, sloužících k vyhodnocení rizik. Dále také budou podrobně vysvětlené jednotlivé hodnoty hrozeb a okomentovaná jejich pravděpodobnost naplnění.

7. Rizika

7.1. Hodnocení rizik

Nyní tedy rizika vyjadřují, která aktiva firmy jsou nejvíce ohrožena a jakou hrozbou.

Postup vyhodnocení rizik byl následující:

1. Vytvořit tabulky hrozeb, které mohou působit na jednotlivá aktiva
2. Vynásobit hodnoty aktiv a hodnoty hrozeb
3. Vytvořit tabulky rizik
4. Okomentovat dílčí výsledky

| Identifikované aktivum | Možné hrozby |
|---------------------------------------|--|
| Podnikové informační systémy | Chyba správce; Chyba uživatele; Kyberterorismus; Použití škodlivého SW; Selhání HW |
| Webové stránky | Chyba správce; Kyberterorismus; Selhání sítě |
| Notebooky, tablety, stolní PC | Požár; Výpadek el.proudu; Chyba správce; Chyba uživatele; Selhání HW |
| Tiskárny, klávesnice, myši a další HW | Požár; Selhání HW; Chyba uživatele |
| PC stojany v lékárnách | Selhání SW; Selhání HW |
| Servery | Požár; Výpadek el.proudu; Chyba správce; Kyberterorismus; Selhání HW |
| Telefony - přístroje | Požár; Odposlouchávání |
| Budovy | Požár |
| Lidé | Požár |

Tabulka 7.1.a Hrozby, které ohrožují jednotlivá aktiva

Nyní jsem vynásobil "hodnoty – škály aktiv" (viz. Tab. 5.8.) a "hodnoty – škály hrozeb" (viz. Tab. 6.2.). Na každé aktivum může působit více hrozeb. Spočítal jsem tedy jednotlivá rizika. I když na každé aktivum působí více hrozeb zároveň, tak jako riziko budu uvažovat právě největší možný součin, tedy největší riziko, které může nastat. Je to logické, protože největší hodnoty jsou u nejvíce důležitých aktiv pro chod podniku a u nejpravděpodobnějších hrozeb, které mohou nastat.

| Identifikované aktivum | Hrozba | Riziko |
|------------------------------|-----------------------|----------|
| Podnikové informační systémy | Chyba správce | 7*8 = 56 |
| Podnikové informační systémy | Chyba uživatele | 7*5 = 35 |
| Podnikové informační systémy | Kyberterorismus | 7*4 = 28 |
| Podnikové informační systémy | Použití škodlivého SW | 7*5 = 35 |
| Podnikové informační systémy | Selhání SW | 7*9 = 63 |

Tabulka 7.1.b Rizika SW systémů

Informační systémy tohoto typu slouží pro komunikaci zaměstnanců s vedením firmy, která takto informuje o případných změnách. Dále jsou tyto systémy využívány pro zadávání dat (finanční data, ujeté kilometry, provolané minuty na mobilních telefonech) do databázových systémů a prohlížení naplánovaných akcí v kalendářové aplikaci. Některé systémy jsou dokonce propojené a slouží jako objednávkový systém, jak je uvedeno dříve v práci. Proto patří toto aktivum k těm nejvíce ceněným pro správný chod podniku. Největším rizikem je tedy selhání některé z aplikací, popřípadě celého systému. Jelikož se zde shromažďují interní data a plánují a analyzují se například schůzky s lékaři, je velmi podstatné umět toto riziko velmi rychle řešit a neodkládat.

| Identifikované aktivum | Hrozba | Riziko |
|------------------------|-----------------|----------|
| Webové stránky | Chyba správce | 5*8 = 40 |
| Webové stránky | Kyberterorismus | 5*4 = 20 |
| Webové stránky | Selhání sítě | 5*7 = 35 |

Tabulka 7.1.c5 Rizika webových stránek

Webové stránky obsahují pouze obecné informace o firmě, o které „hacker“ nejspíše nezavádí ani koutkem oka, proto je pro ně kyberterorismus nejnižším rizikem. Naopak chyba správce, který webové stránky tvoří a edituje, se projeví na první pohled. Webové stránky však rozhodně nejsou pro firmu jedním z klíčových aktiv, takže se před tímto rizikem může upřednostnit například selhání serveru a riziko spojené s webovými stránkami vyřešit později. Největším rizikem působícím na aktivum webové stránky je tedy chyba správce.

| Identifikované aktivum | Hrozba | Riziko |
|-------------------------------|-------------------|------------------|
| Notebooky, tablety, stolní PC | Požár | $2 \cdot 2 = 4$ |
| Notebooky, tablety, stolní PC | Výpadek el.proudu | $2 \cdot 4 = 8$ |
| Notebooky, tablety, stolní PC | Chyba správce | $2 \cdot 8 = 16$ |
| Notebooky, tablety, stolní PC | Chyba uživatele | $2 \cdot 5 = 10$ |
| Notebooky, tablety, stolní PC | Selhání SW | $2 \cdot 9 = 18$ |

Tabulka 7.1.d Rizika Notebooků, tabletů a stolních PC

Vypočítaná rizika spojená s notebooky, tablety a stolními PC mohou být poněkud zavádějící. Z logiky vyplývá, že požár fyzicky ohrožuje veškerý hardware rozhodně více, než jeho singulární selhání, avšak musíme si uvědomit, že riziko je vždy počítáno ze dvou hodnot. V tuto chvíli pro nás důležitější hodnotou je hodnota související hrozby, respektive její pravděpodobnost naplnění. Jednoduše řečeno, je mnohem pravděpodobnější, že některý z mnoha počítačů selže nebo se zničí rukou uživatele, než že budovu firmy zachvátí požár. Když tedy k selhání hardwaru dojde, jednoduše se vymění za jiný kus. Toto riziko je jedno z nejběžnějších, které firma řeší a není na něm nic zásadního. S takovými ztrátami se zkrátka počítá. Největším rizikem, které tedy hrozí hardwaru tohoto typu, je jeho selhání a tím způsobená nečinnost.

| Identifikované aktivum | Hrozba | Riziko |
|---------------------------------------|-----------------|-----------------|
| Tiskárny, klávesnice, myši a další HW | Požár | $1 \cdot 2 = 2$ |
| Tiskárny, klávesnice, myši a další HW | Chyba uživatele | $1 \cdot 5 = 5$ |
| Tiskárny, klávesnice, myši a další HW | Selhání HW | $1 \cdot 9 = 9$ |

Tabulka 7.1.e6 Rizika HW

S vypočítanými riziky v této tabulce je realita stejná jako u předchozího aktiva. Tiskárna je nejčastěji ohrožena fyzickým zničením nebo opotřebením, stejně jako ostatní zmíněný hardware. A proto se s jeho poškozením počítá. Největším rizikem působícím na právě tuto skupinu aktiv je tedy opět jeho fyzické (v případě tiskáren se zabudovaným operačním systémem, je ale nutné počítat i se selháním softwaru) selhání a tím způsobená nečinnost.

| Identifikované aktivum | Hrozba | Riziko |
|------------------------|------------|----------|
| PC stojany v lékárnách | Selhání HW | 2*9 = 18 |
| PC stojany v lékárnách | Selhání SW | 2*9 = 18 |

Tabulka 7.1.f Rizika stojanů v lékárnách

Tyto stojany jsou financované firmou GSK a stojí povětšinou v lékárnách, nebo v prostorách nemocnic. Slouží jako interaktivní průvodce mezi produkty firmy GSK - je to tedy počítač s nastaveným neměnným programem. Když se uvnitř něco poškodí, je to oznámeno technikovi, který se snaží problém co nejdříve vyřešit, ale i před vyřešením tohoto rizika se dá upřednostnit riziko jiné, důležitější. Největším rizikem pro PC stojany je tedy selhání softwaru a HW – hodnota těchto rizik je stejná.

| Identifikované aktivum | Hrozba | Riziko |
|------------------------|-------------------|----------|
| Servery | Požár | 9*2 = 18 |
| Servery | Výpadek el.proudu | 9*4 = 36 |
| Servery | Chyba správce | 9*8 = 72 |
| Servery | Kyberterorismus | 9*4 = 36 |
| Servery | Selhání HW | 9*9 = 81 |
| Servery | Selhání síť | 9*7 = 63 |

Tabulka 7.1.g Rizika serverů

Servery jsou určitě jedním z nejcennějších aktiv. Jsou důležité pro chod všech interních softwarových aplikací a také webových stránek. Není tedy s podivem, že na toto aktivum působí také několik hrozeb, avšak právě kvůli jeho důležitosti je třeba obávat se více z nich. Ať už výpadek proudu nebo chyba některého ze správců může server, který obsahuje důležitá data ohrožit. Největší problém je však se selháním jednoho ze serverů samo o sobě. Disky s daty se nepřetržitým zapisováním dat velmi často rozbijí samy o sobě, pouze následkem dlouhodobého užívání. Proto je nutné umět tento problém řešit rychle a mít připravené okamžité řešení.

| Identifikované aktivum | Hrozba | Riziko |
|------------------------|-----------------|----------|
| Telefony – přístroje | Požár | 4*2 = 8 |
| Telefony - přístroje | Odposlouchávání | 4*4 = 16 |

Tabulka 7.1.h Rizika pevných telefonů

Těmito přístroji se myslí kancelářské pevné linky. Kromě fyzického porušení je rizikem také odposlouchávání rozhovorů. Tato hrozba je v práci uvedena na základě konzultace s pracovníkem GSK, který nás informoval, že pobočka firmy GSK se sídlem v Londýně má přímo s odposloucháváním pevných linek zkušenosti, proto tedy toto riziko opravdu hrozí.

| Identifikované aktivum | Hrozba | Riziko |
|------------------------|--------|---------|
| Budovy | Požár | 6*2 =12 |

Tabulka 7.1.i Rizika budov

Budovy patří mezi nejstálejší aktiva. Ovšem když už je hrozba naplněna, může způsobit finančně velmi závažné škody. Jejich poškození je velmi nepravděpodobné, protože riziko je většinou spojeno s nějakou přírodní katastrofou. Nejpravděpodobnější a také jedinou hrozbou je požár.

| Identifikované aktivum | Hrozba | Riziko |
|------------------------|--------|----------|
| Lidé | Požár | 9*2 = 18 |

Tabulka 7.1.j Rizika lidí

Lidé rozhodně patří mezi nejdůležitější aktiva firmy, dokonce jsou snad tím vůbec nejpodstatnějším. Z logiky plyne, že bez personálu žádný podnik ani nevznikne. I když se může zdát zkoumání rizik takového aktiva irelevantní, tak i lidé jsou součástí informačního systému a hrozby na ně působí. Jejich naplnění je ovšem dosti nepravděpodobné. Jako nejvyšší riziko tedy znovu vyšel požár.

Nyní jsou známa všechna rizika, jež mohou postihnout jednotlivá aktiva našeho zkoumaného podniku. Tím ale práce nekončí. Ve chvíli kdy rizika vyplují na povrch, je nutné umět je řešit, jak bylo řečeno v teoretické části této práce. Řešením by mohl být souhrn bezpečnostních opatření, která se pokusím osobně sestavit a udělat z něj tak vlastní přínos k této práci.

8. Bezpečnostní opatření

Nejlepší způsob řízení rizik je předejít potencionálním hrozbám dříve, než nastanou, nebo se o tuto skutečnost alespoň snažit, protože ne vždy je to reálné (některé z hrozeb jednoduše musí nastat, aby se o nich vůbec vědělo, a řeší se zpětně). Výborným řešením této situace jsou navrhovaná bezpečnostní opatření a jejich dodržování.

8.1. Navrhovaná opatření pro jednotlivá rizika

8.1.1 Požár a výpadek elektrického proudu

Proti požáru je obecně těžké podnik ochránit. Nelze mu předejít a škody jsou ničivé. Nabízí se však hned několik opatření:

- zajištění bezpečných, dobře označených únikových cest z budov (evakuační plán).
- udržování varovných systémů ve stálé pohotovosti, tím, že se ve stejných časových intervalech zkouší jejich provoz.
- proškolení personálu, jak musí v podobných situacích jednat.

Používání systémů podobného typu i v prostorách laboratoří a výzkumných centrech, kde může dojít k průmyslové havárii.

Pro případy výpadku el.proudu slouží zařízení zvané UPS, *které zajišťuje souvislou dodávku elektřiny pro zařízení, která nesmějí být neočekávaně vypnuta. UPS je obvykle zapojen mezi primární zdroj elektřiny a vstup napájení chráněného zařízení, viz [5].* Dají se tak uchránit důležitá data.

8.1.2 Chyba správce, chyba uživatele

Selhání lidských zdrojů je běžnou součástí řízení rizik. Předcházet jim a eliminovat je ve velkém množství lze vhodným výběrem uchazečů o pracovní pozice, tvrdšími nároky na zkušenosti a pracovní morálku. Tímto se myslí například fakt, že správce sítě musí být k zastížení nonstop a měl by být schopen nárazově řešit způsobené výpadky. Správců by mělo být více a každý by se měl soustředit pouze na svou určenou oblast, tím se také

eliminuje většina chyb. Osobně si totiž myslím, že většinou vznikají chyby správce či uživatele jejich přílišným zatížením.

Dále je nezbytné všechny pracovníky průběžně proškolovat, aby nedocházelo ke zbytečným chybám. Zaškolení by mělo být jednou z náplní práce správce, který se pohybuje přímo ve firmě. Dalším řešením vedoucím k zamezení rizik této třídy, je nutnost motivovat zaměstnance k ochraně svěřeného majetku finanční spoluúčástí na jeho poškození.

8.1.3 Kyberterorismus

S vývojem informačních technologií obecně, se vyvíjí svět kyberterorismu a přináší stále větší hrozby pro jednotlivce, ale především firmy a podniky, které prosperují. Aktualizovaný antivirový systém jednoznačně chrání počítače a je opravdu nezbytnou součástí, která chrání aktiva firmy před napadením nežádoucím softwarem. Dalším prostředkem pro ochranu před hackery jsou stále se vyvíjející routery, které mají schopnost poznat, že jiný počítač se do sítě snaží příliš často získat přístup. Pokud router takovou aktivitu zaznamená, jednoduše zakáže danému zdroji přístup do sítě. Pokud by měla firma potřebu chránit se lépe, je vhodné najmout specialistu na problematiku spojenou s kyberterorismem, který je rozpoznat nežádoucí aktivitu.

8.1.4 Odposlouchávání

Výskyt odposlouchávání mobilních telefonů nebo pevných linek v kancelářích není nijak raritní záležitostí. Naštěstí existují metody, jak se hrozbě odposlechů bránit. Způsobů je hned několik. Například generátory šumu, které do telefonního přenosu přimíchají jakýsi "šum" a hovor pak není možné rozpoznat. Dále existují radiové analyzátoři. Tato zařízení mají schopnost vyhodnotit, že zkoumaný signál obsahuje navíc nežádoucí aktivitu. Existují také fólie a tapety na zdi místnosti, která ji přemění v tzv. Faradayovu klec, která zamezí do místnosti přístup radiových signálů, viz [6].

8.1.5 Použití škodlivého softwaru

Škodlivý software se myslí software napadený počítačovými viry, kterých je mnoho druhů. Použití škodlivého softwaru je ve většině případů chyba uživatele, který nemá

tušení, že otevírá soubor, který je právě napadený. Řešením je proto předejít události a nedat uživateli možnost s infikovanými soubory zacházet. To se dá vyřešit opět nasazením antivirových systémů a také tím, že zaměstnanci budou do firemní sítě přistupovat pouze skrze firemní přístroje s uzavřenou politikou. Samozřejmě ale existuje obecnější řešení ve smyslu zabezpečení přímo firemní sítě, jejíž přístupový bod bude kontrolovat bezpečnostní software a filtrovat podezřelé přístroje.

8.1.6 Selhání softwaru, selhání hardwaru, selhání sítě

Selhání softwaru lze předejít především aktualizacemi systému a jejich častými kontrolami. Aktualizace jsou proto nezbytným prvkem proti selhání softwaru. Dalším faktorem spolehlivosti softwaru je rozhodně výběr spolehlivých dodavatelů. Ideální jsou proto dodavatelé od světových firem, které jsou zárukou kvality a spolehlivosti. Firma by se měla snažit finančně podporovat celý systém informačních technologií. Snažit se v tomto směru příliš šetřit není vhodným krokem na cestě spolehlivého chodu informačních systémů.

K selhání hardwaru je vhodné zmínit pojem interní databáze firmy a zvláště jednotlivé disky, které slouží k uchování veškerých potřebných dat. Tyto disky se čas od času poškodí a je nutné mít vždy připravený určitý počet disků záložních určených k výměně těch poškozených, aby se nově zapsaná data neztrácela.

Hardwarovou aktualizaci lze chápat jako nahrazování přístrojů novějšími, tím i bezpečnějšími. I zde je ovšem velmi důležitý výběr dodavatele, lépe řečeno důležitější než u softwaru.

Proti selhání sítě se dá předcházet výběrem specializovaného pracovníka, tedy administrátora, který bude mít přehled o veškerém dění v síti a bude analyzovat aktivitu. Správce sítě je proto klíčovým aktivem, které zamezuje vzniku rizika ohrožujícího firemní síť.

9. Závěr

Cílem této práce je vyřešení přehledné studie finanční analýzy a praktického příkladu analýzy rizik informačního systému a s tím spojených informačních technologií v konkrétní firmě.

Teoretické poznatky analýzy rizik IS byly aplikovány na konkrétní firmu, která se zabývá výzkumem a prodejem farmaceutických produktů. GlaxoSmithKline, s.r.o., je pobočkou jedné z největších farmaceutických firem na světě GlaxoSmithKline Plc., která sídlí v Londýně. Protože zdroje dat potřebných pro komplexní analýzu rizik jsou u této konkrétní firmy velmi omezené, nemohl jsem strukturu analýzy volit tak, abych z minima dat získal odpovídající obraz rizik. Oficiálně jsou dostupné informace z finančního účetnictví ve formě výročních zpráv, viz Obchodní rejstřík. Proto jsem do analýzy rizik zařadil analýzu finančního zdraví společnosti. Motivací je fakt, finanční nedostatky firmy mohou vyvolat problémy s financováním pořízení a provozu IS. Výsledkem finanční analýzy je však skutečnost, že firmě finanční rizika skoro nehrozí a jeví se jako finančně velmi stabilní.

Dále jsem analyzoval rizika plynoucí z finančních ztrát při výpadku modulu IS EPOS, který je objednávkovým modulem IS. Zde je proveden odhad možných finančních dopadů denního výpadku systému.

Poté se v analýze rizik vyhodnotila jednotlivá aktiva firmy a hrozby, které na ně působí a vypočítala se z nich celková rizika.

Poslední bod této práce patří stanovení seznamu bezpečnostních opatření, která chrání aktiva před nežádoucími vlivy, čímž se dospělo až k tomuto závěru.

Přílohy:

CD s vypracovanou finanční analýzou.

Seznam použitých zdrojů:

- [1] SODOMKA, P. *Informační systémy v podnikové praxi*. Vyd. 1. Brno: Computer Press, 2006. ISBN 80-251-1200-4.
- [2] BASL, J. *Inovace podnikových informačních systémů: podpora konkurenceschopnosti podniků*. 1. vyd. Praha: Professional Publishing, 2011. ISBN 978-80-7431-045-4.
- [3] *Podnikové informační systémy*. [online – 23.3.2014] Dostupné z: <http://www.root-it.cz/podnikove-informacni-systemy.aspx>
- [4] ADÁSKOVÁ, P. *Systematický přístup k výběru vhodné metody analýzy rizik v organizaci*. [online – 12.3.2014]. Dostupné z: <http://www.risk-management.cz/tisk.php?clanek=3727>
- [5] UPS. [online – 5.4.2014]. Dostupné z: <http://www.hd.cz/rady/zalozni-zdroje-ups.php>
- [6] KUČERA, F. *Mobilní odposlechy – jak fungují a lze se jim bránit?*. [online - 19.3.2014]. Dostupné z: <http://www.svetandroida.cz/mobilni-odposlechy-jak-funguji-a-lze-se-jim-branit-201201>
- [7] KOČMANOVÁ, A., LUŇÁČEK, J. *Ekonomika podniku 2.díl* Brno: VUT v Brně, fakulta podnikatelská, 2005. ISBN 80-214-3017-6.
- [8] ŠIMKOVÁ, K. *Finanční analýza a mezinárodní účetní standardy*. Plzeň, 2010. Bakalářská práce na Fakultě aplikovaných věd Západočeské univerzity v Plzni. Vedoucí bakalářské práce Ing. Pavel Nový, PhD.
- [9] SEQUENS, L. *Analýza vlastností Tafflerova bankrotního modelu*. Plzeň, 2007. Bakalářská práce na Fakultě aplikovaných věd Západočeské univerzity v Plzni. Vedoucí bakalářské práce Ing. Pavel Nový, PhD.
- [10] ŽIŽKA, J. *Analýza vlastností Kralickova Quick Testu*. Plzeň, 2009. Bakalářská práce na Fakultě aplikovaných věd Západočeské univerzity na katedře informatiky a výpočetní techniky. Vedoucí bakalářské práce Ing. Pavel Nový, Ph.D.

- [11] VOŘÍŠEK, J. *Kritické faktory úspěchu a rizika informačních systémů*. [online – 11.4.2014]. Dostupné z:
http://nb.vse.cz/~vorisek/FILES/Clanky/1996_Csf_a_rizika_IS.htm
- [12] VANÍČEK, J.; PAPÍK, M.; PERGL, R.; VANÍČEK, T. *Teoretické základy informatiky*. Praha. Kernberg Publishing. 2007. ISBN 978-80-903962-4-1
- [13] BRADA, P. *Data, informace, znalosti a jejich předávání* [online – 20.3.2014] 2012, Dostupné z: Courseware ZČU- Znalostní a informační management- Data, informace, sdílení znalostí.pdf
- [14] Obrat aktiv. [online – 11.5.2014]. Dostupné z:
<https://managementmania.com/cs/obrat-aktiv>
- [15] Poměr vlastního kapitálu a celkových aktiv. [online – 19.5.2014]. Dostupné z:
<https://managementmania.com/cs/pomer-vlastniho-kapital-a-celkovych-aktiv>
- [16] Benchmarking. [online – 12.4.2014]. Dostupné z: <http://www.mpo.cz/cz/infa.html>
- [17] Sunsystems. [online - 5.6.2014]. Dostupné z:
http://www.systemonline.cz/prehled-informacnich-systemu/ekonomicke-systemy/infor-sunsystems-1.htm?razeni=d_d_d&dalsi=&dalsi_main=0&dalsi_more=
- [18] EPOS. [online – 5.6.2014]. Dostupné z: <http://www.epos.cz/obis4/schema.html>
- [19] TREX. [online - 6.6.2014]. Dostupné z: http://www.comparex-group.com/MediaLibrary/Content/web/cz/cz/topics/focus_topics/development_standard_software/boss/BOSS_TREX_letak.pdf
- [20] CITIBANK. [online – 6.6.2014]. Dostupné z:
http://www.citi.com/czech/gcb/corporate_banking/czech/medium_companies_static/internetove_bank.htm
- [21] HELIOS. [online – 6.6.2014]. Dostupné z:
<http://www.helios.eu/fenix/funkcionalita/ekonomicky-subsystem/majetek.html>