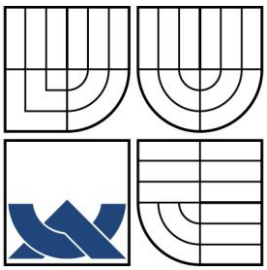
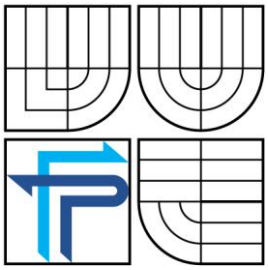


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA PODNIKATELSKÁ
ÚSTAV MANAGEMENTU

FACULTY OF BUSINESS AND MANAGEMENT
INSTITUT OF MANAGEMENT

PODNIKATELSKÝ PLÁN

BUSSINESS PLAN

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — Bc. IVAN NOVÁK
AUTHOR

VEDOUCÍ PRÁCE — doc. Ing. ALENA KOCMANOVÁ, Ph.D.
SUPERVISOR

BRNO 2009

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2008/2009
Ústav managementu

ZADÁNÍ DIPLOMOVÉ PRÁCE

Novák Ivan, Bc.

Řízení a ekonomika podniku (6208T097)

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách, Studijním a zkušebním řádem VUT v Brně a Směrnicí děkana pro realizaci bakalářských a magisterských studijních programů zadává diplomovou práci s názvem:

Podnikatelský záměr

v anglickém jazyce:

Business Plan

Pokyny pro vypracování:

Úvod
Vymezení problému a cíle práce
Teoretická východiska práce
Analýza problému a současné situace
Návrh podnikatelského záměru
Financování a rizika projektu
Zhodnocení realizace podnikatelského záměru
Závěr
Seznam použité literatury
Přílohy

Seznam odborné literatury:

FOTR,J.Podnikatelský záměr a investiční rozhodování.1vyd.Praha:Grada.2005.356s. ISBN 80-247-0939-2
SYNEK,M.Ekonomická analýza.1.vyd.Praha:Oeconomica.2004.79s. ISBN 80-245-063-3
WUPPERFELD,U.Podnikatelský plán pro úspěšný start.Praha:Management Press.2003.160s. ISBN 80-7261-075-9

Vedoucí diplomové práce: doc. Ing. Alena Kocmanová, Ph.D.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2008/2009.

L.S.

PhDr. Martina Rašticová, Ph.D.	doc. RNDr. Anna Putnová, Ph.D., MBA
Ředitel ústavu	Děkan fakulty

V Brně, dne 03.04.2009

ABSTRAKT (ANOTACE)

Předmětem této diplomové práce je zpracování podnikatelského záměru pro zavedení nového informačního systému pro státní správu, s vyhodnocením a s posouzením zda podnikatelský záměr přijmout či zamítnout. Posouzení podnikatelského záměru je použitím metod analýzy, metrik pro informační systémy.

ABSTRACT (ANNOTATION)

The subject of this thesis is the processing of the business plan for the introduction of a new information system for the administration, with an evaluation and with an assessment whether the business plan to accept or reject. Assessment of business plan is to use methods of analysis, metrics for information systems.

KLÍČOVÁ SLOVA:
Podnikatelský záměr; Standardy NBÚ; Standardy NATO; Efektivní investice; Čistá současná hodnota, Doba návratnosti investice;

KEYWORDS:
Business plan; Norm of NBÚ (Czech National security agency); Norm of NATO; Investment efficiency; Net present value; Pay back investment;

BIBLIOGRAFICKÁ CITACE

NOVÁK, I. *Podnikatelský záměr*. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2009, 106 s. Vedoucí diplomové práce doc. Ing. Alena Kocmanová, Ph.D.

ČESTNÉ PROHLÁŠENÍ

Prohlašuji, že předložená diplomová práce je původní a zpracoval jsem ji samostatně.

Prohlašuji, že citace použitých pramenů je úplné, že jsem v práci neporušil autorská práva (ve smyslu zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 15. května 2009 ……

Bc. Ivan Novák

PODĚKOVÁNÍ

Na tomto místě bych chtěl poděkovat doc. Ing. Aleně Kocmanové, Ph.D. za cenné připomínky a spolupráci, kterými přispěla k zdárnému dokončení práce.

V Brně dne 15. května 2009 ……

Bc. Ivan Novák

Obsah:

Úvod, vymezení problémů a cíl práce

Ve své diplomové práci se zabývám návrhem na **„Podnikatelský záměr[4] s vyhodnocením jeho doporučením k realizaci nebo případným zamítnutím na základě analýz“.** Podnikatelský záměr bude směřovat do státní správy, oblasti vybudování komunikačního a informačního systému nakládajícího s utajovanými informacemi do stupně „DŮVĚRNÉ“ a pracujícího s daty a informacemi on-line.

Podnikatelský záměr je jednou ze základních a nejdůležitějších úvah při realizaci a rozvoji projektu, je to dlouhodobý a finančně náročný projekt, který na dlouho dobu ovlivní směr, technický vývoj a finanční zatížení, určí výběr technologie, výběr lidských zdrojů na jeho provozování a v neposlední řadě i ovlivní mnoho pracovních a kolegiálních vztahů. Tento projekt je nutno podrobit mnohým analýzám, jak po stránce ekonomické, personální, administrativní, fyzické bezpečnosti, tak i informačních systémů, na technologii a všechny související parametry projektu je nutné podrobit a implementovat matematicko – statistické metody, analýzy či metriky.

Práci jsem rozdělil do několika sofistických celků, které na sebe navzájem navazují a vytváří jednotný moderní informační systém, který je nutno vybudovat, finančně a ekonomicky zainventovat a na základě analýz a metrik doporučit či zamítnout.

Při projektu jsem byl nucen nastudovat mnoho materiálů, které se zabývají ochranou utajovaných informací [30],osobních údajů[29] včetně podpůrných zákonů, vyhlášky NBÚ[37], [38], [39], [40], [41], standardy NATO[1][22] a doporučení státy EU[2][23], Jedná se o informační systémy, které propojují citlivá centra pro boj s organizovaným zločinem, s mezinárodními daňovými úniky a v neposlední řadě s terorismem.

V každé kapitole projektu je teoretické východisko, opřené o studium výše popsaných materiálů. Výsledky jsou podepřeny analýzami nebo metrikami problému a vyhodnocením každé kapitoly.

[1] SNAC – Systém and Network Attack Center
[2] ISO/IEC 17799

V závěru diplomové práce jsou shrnuty všechny výsledky a podnikatelský záměr je doporučen či zamítnut k realizaci s odůvodněním.

Informační a komunikační systémy ve státní správě byly budovány v 90. letech minulého století Tomuto období odpovídá hardware a software, technické, objektové, administrativní i personální zabezpečení těchto systémů. Rozhodnutí o inovaci bylo velmi náročné a opíralo se o současné potřeby státní správy na zajištění ochrany utajovaných informací pro všechny ministerstva a resorty České republiky, které přicházejí do styku s utajovanými informacemi.

Vybudování moderních informačních a komunikačních systémů je jedním z nejdůležitějších předpokladů prosperity a identity České republiky. Veškeré poznatky využívané při rozhodovacích procesech v oblasti teoretické, praktické i technické vycházejí z dlouholeté odborné praxe v oboru a zkušenosti pracovníků podílejících se na řešení problematiky.

Pro podnikatelský záměr jsem se rozhodl na základě informací a potřeb, které přicházeli ze sféry státní správy. V současné době nedisponuje kompatibilním informačním a komunikačním systémem on-line od stupně utajení „VYHRAZENÉ“ a vyšší. Určitě existuje mnoho sofistikovaných firem, které se touto oblastí zabývají, jsou ekonomicky, technicky a personálně mohutnější, ale jejich nevýhodou jsou vysoké fixní i variabilní náklady a tím vysoká cena za koncový produkt a službu.

Střední podniky v současném tržním hospodářství mají nezastupitelné místo, přesto že mají svoji pozici na trhu velmi těžkou, neboť se musí potýkat s řadou nevýhod, jak z oblasti ekonomické, personální, vědecko-technické a legislativně-právní. Velké a zahraniční firmy mají na každou oblast specializovaná logistická oddělení, avšak za cenu vyšší nákladů.

Každý komunikační i informační systém budovaný v určitém čase a za určitých podmínek je certifikován NBÚ na určitou dobu. Je vydáván „CERTIFIKÁT NA PROVOZOVÁNÍ“. Je nutné ho pravidelně obnovovat, doplňovat podle podmínek doby a podle situací v oblasti ochrany utajovaných informací.

Oblast ochrany informací se velice dynamicky rozvíjí. V 90. letech minulého století byly hlavních přenosovým mediem pro tyto systémy byly, speciální telefonní přístroje, faxová spojení a hardwarové šifrovací stroje[5]. V 21. století, v době počítačové expanze, se ochrana informací a komunikací přesunuje do oblasti automatických systému řízení [3]. Toto jsou „informační systémy, které nás obklopují a pro jejichž činnost je využívaná v převážné většině výpočetní technika založena na „Personal computer“ (dále jen „PC“) s podpůrnými programy a výstupními periferiemi.

Informační a komunikační systémy nemusí být podporovaný výpočetní technikou, a je lhostejné, zda je systém automatický (použití strojového zpracování) nebo neautomatický (papírová kartotéka), ale vždy musí splňovat podmínky na ochranu citlivých a osobních informací. Příkladem informačního systému může být telefonní seznam, knihy příchozí pošty, evidence osob nebo také účetnictví, kalkulace a investiční záměry.

Tabulka č.1: Definice informačního systému

Identifikační funkční celek zabezpečující cíle, vědomé a systematické shromažďování, zpracovávání, uchovávání a zpřístupňování informací uložených na hmotném nosiči v údajových základnách reprodukovatelných technickými prostředky. Informační systém integruje (zahrnuje) informační základnu (data), technické a programové prostředky, technologie, finanční prostředky a lidské zdroje.	Standardy státního informačního systému ČR (ÚSIS Praha, prosinec 1996, 1. díl, s. 63)
Systém zpracování informací spolu s návaznými organizačními prostředky, např.: personálem, technickými a finančními, takový systém získává a distribuuje informace.	Norma ČSN ISO/IES 2382-1. Informační technologie – Slovník, část1: Základní termíny
Systém, v němž vazby mezi prvky se chápou jako informace (data), resp. směry jejich toků a jednotlivé prvky jako místa vzniku, předzpracováním, přenosu, uchování, zpracování, distribuce či zániku informací (dat); jeho účelem je tvorba prezentace informací	Systémové nástroje řízení *(Veselý, J., Praha 1982, s.302)*

[3] Vyhláška Státní komise pro vědecký a investiční rozvoj č.57/1986 Sb., o budování automatických systémů řízení

Funkční celek zabezpečuje cílevědomé a systematické shromažďovaní, zpracovávání, uchovávání a zpřístupňování informací. Každý informační systém zahrnuje informační základnu, technické a programové prostředky, technologie, finanční prostředky a lidské zdroje.	§4 zákona č. 101/2000 Sb., o ochraně osobních údajů v informačních systémech

Zdroj: Smejkal. V., a kol.: „Právo informačních a telekomunikačních systémů“, s. 42

V předcházející tabulce je jen několik definic jak vymezit informační systém, jak chápat spojení „železa“, „myšlenky“ a člověka, jejich souvztažnost, propojení, odpovědnost, bezpečnost a loajálnost.

Informační systém podporovaný výpočetní technikou se skládá z následujících komponentů:

- **Technické prostředky** – hardware – počítačové sestavy, včetně výstupních periferních jednotek (multifunkční zařízení, zálohovací pole a databanky),
- **Programové prostředky** – software – programové vybavení, které řídí chod počítače, slouží k efektivnímu zapracovávání a vytěžování dat v informačním systému, komunikace informačního systému v interní síti, komunikaci s reálným světem – Internet, aplikačními programy,
- **Datové zdroje** – k práci s daty v informačním systému se využívají programové prostředky,
- **Organizační prostředky** – orgware – soubor nařízeních a pravidel pro provozování a využívání informačního systému v rámci společnosti, zamezující úniku dat a citlivých informací,
- **Lidské zdroje** – peopleware – účinné fungování lidských zdrojů v informačních systémech.

Pojem **„informační systém“**[8] bývá v praxi chápán velmi různě. Většina veřejnosti si jej nesprávně ztotožňuje s využíváním programů, které evidují a zpracovávají určitá data. V literatuře najdeme celou řadu definic např., ty které můžeme shrnout do následující podoby[1]:

...„Informační systém je spojení hardware, software a orgware, a jeho cílem je zpracování a uchování informace k zvýšení efektivnosti lidské činnosti“...

Cíl práce je navrhnout funkční kompatibilní on-line systém spojený s využíváním výpočetní techniky pomocí sítě LAN. Všechny informační a komunikační prostředky systému musí komunikovat pomocí TP/IP protokolu[2]. Při komunikaci mezi uživateli musí být zajištěna důvěrnost a integrita informace, všude kde je tato funkce potřeba musí být systémem poskytnuta při zajištění odpovědnosti uživatele systému za všechny jeho činnost konané v systému.

Cílem diplomové práce je návrh komunikačního a informačního systému a vyčíslení investic do takového projektu, který musí splňovat vysoké technické nároky, minimální poruchovost, možnost přechodu na záložní systém, kompatibilitu se státy Evropské Unie, kompatibilitu se složkami NATO i se standardy NBÚ. Úkolem koncepce utajeného spojení je vybudovat jeden informační systém ve státní správě pro přenos utajovaných informací od stupně utajení „VYHRAZENÉ“, ve kterém by bylo možno přenášet hlas, data a video.

K zajištění důvěrnosti a integrity přenášených utajovaných informací bude použit IP kryptografický prostředek umožňující přenos utajovaných informací národních, NATO a EU. Systém bude umožňovat propojení uživatelů ze systému používaných i Emini státními složkami, které budou investovat do kompatibilního systému spojení.

Navržený informační a komunikační systém pro státní právu, který bude zpracovávat, ukládat, využívat a vytěžovat data a informace on-line a pro společnost, která tuto zakázku vyhraje, přinese maximální finanční užitek, konkurenční výhodu na trhu služeb v této oblasti a zajistí na dlouhou dobu prospěch společnosti, sociální zabezpečení zaměstnancům a jejich rodinám. Návrh komunikačního a informačního systému je nutno podrobit podrobné analýze všech komponentů. Investice do takového projektu budou nemalé a lze tento projekt financovat ze státního rozpočtu České republiky, případně z programů PHARE pro země Evropské unie. Systém musí splňovat vysoké technické nároky, maximální bezpečnost informací, minimální poruchovost, možnost přechodu na záložní systém, kompatibilitu se státy Evropské Unie[34], [35], [36] se složkami NATO i se standardy NBÚ[37], [38], [39], [40], [41].

Zpracovávání utajovaných informací a dat v systému a vlastní systém je navržen tak, aby byl provozován v souladu se zákonem č. 412/2005 Sb.[30], o ochraně utajovaných informací a o bezpečnostní způsobilosti a vyhláškou Národního bezpečnostního úřadu č. 523/2005 Sb., o bezpečnosti informačních systémů a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor a všech zákonů a nařízení NBÚ[37], [38], [39], [40], [41] a standardů NATO[22][4].

Návrh bezpečnosti systému obsahuje popis způsobu realizace jednotlivých bezpečnostních požadavků vzniklých při analýze rizik systému ve formě bezpečnostních opatření, bezpečnostních funkcí a bezpečnostních mechanizmů. Základním požadavkem je vytvořit bezpečné podmínky pro nakládání s neutajovanými informacemi a utajovanými informacemi do stupně utajení „Vyhrazené“ v systému.

Dalším požadavkem spojeným s využíváním systému je zajištění takového řešení bezpečnosti, které nebude vyžadovat neúměrně komplikovanou obsluhu počítače a finanční náročnost. Musí být analyzována, měřena metrika a nebude neúměrně zatěžovat uživatele dodatečnými činnostmi nad rámec jeho nutných úkonů při obsluze.

Bezpečné zpracování utajovaných informací je spojeno se zajištěním jejich důvěrnosti a integrity všude, kde se tyto informace vyskytují, dostupnost těchto informací a služeb systému a odpovědnosti uživatele systému za jeho činnost v něm a za ochranu utajovaných informací.

Systém je složen z řídícího pracoviště a ze samostatných lokalit, připojených po síti LAN a WAN[2]. Součástí těchto služeb je provoz dohledových nástrojů a vykonávání bezpečnostního dohledu. Posláním pracovišť umístěných v lokalitách je umožnění uživatelům přistupovat k těmto službám.

Při zpracování práce byly použity analytické, statistické, matematické metody a metriky používané v ekonomickém a investičním rozhodování ve vyspělé tržní ekonomice, k získání kvantitativních a kvalitativních hodnot pro kvalifikované rozhodnutí zda podnikatelský záměr přijmout či zamítnout.

[4] Guide to Securing Microsoft Windows XP „ Operational Network Evaluations Division of the Systems and Network Attack center (SNAC)

1. Teoretická východiska práce

V moderní společnosti 21. století je on-line komunikace pomocí komunikačních a informačních systémů samozřejmostí. Bezpečnost lze zajistit pouze pomocí bezpečné datové sítě s hardwarovou a softwarovou nadstavbovou a šifrovacími produkty a algoritmy. Mnoho uživatelů si neuvědomuje nebezpečnost kdy, kdo a jak jsou jejich data v digitálním světě využívána a zneužívána nepřítelem, konkurencí či jen ze škodolibosti neloajálním zaměstnancem. Znalost těchto základních bezpečnostních zásad a soborů bezpečnostních opatření a použití kryptografie je pro člověka a firmu pohybující ve světě on-line komunikace samozřejmostí a nutností.

Bezpečná komunikační datová síť[6] pro on-line spojení není jen technické řešení systému, ale je to soubor personální, objektové, informační administrativní a manažerské činnosti a uvědomělosti o nebezpečnosti, destruktivnosti a konkurenční výhodě nepřítele, konkurence, záškodníka, který se řídí, poškozuje a prosazuje zájmy cizího subjektu, většinou za značnou úplatu v neprospěch chráněného zájmu a organizace.

Současné komunikační a informační systémy ve státní správě utajeného spojení již nevyhovují dnešním požadavkům na přenos utajovaných a citlivých informací, a to zejména v objemu přenášených dat a jejich utajení pomocí aplikačních prostředků. Použitá technologie současných kryptografických prostředků ve státní správě pro ochranu utajeného spojení je morálně i technicky zastaralá, a již nejsou dostupné komponenty na jejich opravu, obnovu, rozšiřování a preventivní údržbu.

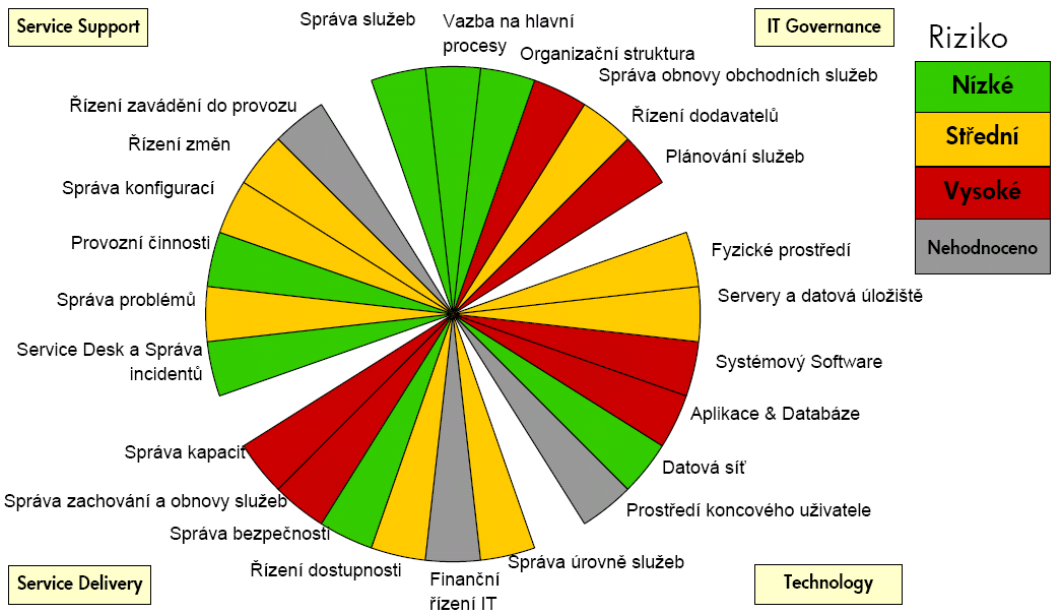
Teoretickým východiskem je vybudovat jeden mohutný implementací robustní systém, který nahradí několik různých nekompatibilních satelitních systému pracujících a provozovaných ve státní správě. Tento systém musí odolávat jak vnějším i vnitřním okolnostem působící na systém, z hlediska existence hrozeb, mír rizika a realizací nutných protiopatření. Všechna tato opatření musí být realizována s maximálním komfortem pro uživatele, v souběhu s maximální účinností proti hrozbám a rizikům, ale s minimálními ekonomickými náklady, které budou státní správu zatěžovat.

Informační a komunikační bezpečnost je technicky, administrativně a personálně velmi náročný obor. Je to obor velmi mladý, ale všude přítomný, dynamicky se

rozvíjející a prakticky nepostradatelný pro současnou komunikaci mezi subjekty, které spolu obchodují, investují do projektů, vyměňují si informace a uzavírají smlouvy či zajišťují mezinárodní bezpečnost proti terorismu. Pracovníci těchto systémů musí být technicky, právně i administrativně velice zdatní a výkonní, ale asi největším požadavkem je bezpečnostní loajálnost ke správě, která tyto systémy spravuje, provozuje a udržuje.

Technicko vědecký, dynamický rozvoj počítačového, komunikačního průmyslu klade na tyto systémy vysoké nároky na obnovu, správu a prevenci proti vnitřním i vnějším útokům, které jsou vždy o krok napřed. Bezpečností a prevencí a souborem opatření lze tento handicap anulovat či být o krok napřed před hrozbou či útokem. V příloze č. 1 diplomové práce je vyjmenováno několik základních názvosloví bezpečnosti komunikačního a informačního systému.

Graf č.1: Znázorňuje rizika v komunikačním a informačním systému



Zdroj: Copyright © 2003 HP corporate presentation ALL rights reserved 2/6/2006

Teoretické východisko diplomové práce je podrobná a systémová analýza stávajících lokálních komunikačních a informačních systému státní správy. Současná státní správa používá tři oddělené OFF-LINE systémy:

1.1 První systém

Prvním systémem je telefonní spojení, které je určeno pro přenos hlasových zpráv s omezeným textově-faxovým spojením s omezeným počtem členů managementu. Důvěrnost a integrita utajovaných informací při jejich přenosu je zajištěna certifikovaným analogovým kryptografickým prostředkem. Využívaný certifikovaný prostředek byl nasazen v roce 1992, jeho pořizovací hodnota činila 243 000,-Kč. Jedná se o lokální zařízení a tudíž musí být u každého uživatele nainstalováno. V rámci tohoto systému je provozováno cca 500 ks zařízení o celkové hodnotě toho 12 150 000,-Kč a dispečerské pracoviště v hodnotě 2 000 000,-Kč[5].

1.2 Druhý systém

Druhým systémem je plnohodnotné faxové spojení. Přenos je zajištěn certifikovaným kryptografickým prostředkem schváleným NBÚ, použitý kryptografický prostředek je morálně i technicky zastaralý. I tento systém je vybaven lokálním prostředkem, který byl nasazen v roce 1995, jeho pořizovací hodnota činila 85 000,-Kč. Jedná se o lokální prostředek a tudíž musí být u každého uživatele nainstalován. V rámci tohoto systému je provozováno cca 50 ks zařízení o celkové hodnotě toho 4 250 000,-Kč.

1.3 Třetí systém

Posledním systémem je „Datové spojení“, které je určeno pro přenos informací (off-line). V současné době je možno data zpracovávat a vyhodnocovat na samostatných PC sestavách. Pro on-line přenos je využívána symetrická šifra s mocností klíče 64 bitů. I tento systém je vybaven lokálním prostředkem, který byl nasazen v roce 2000, jeho pořizovací hodnota činila 15 000,-Kč. Jedná se o lokální prostředek a tudíž musí být u každého uživatele instalován. V rámci tohoto systému je provozováno cca 1 000 ks zařízení o celkové hodnotě toho 15 000 000,-Kč.

[5] Toto odpovídá pouze pokud s časem neklesá hodnota zařízení, v uvedeném případě zařízení odpovídá.

Tabulka č.2: Identifikace nákladů na systémy provozované státní správou

	Celková hodnota zařízení [mil.]	Fixní náklady				Variabilní náklady		
		Spotřeba el. energie	Náklady objektové	Náklady admin.	Mzdové náklady	Náklady servisní	Náklady školení	Certifikační náklady
Systém první	14,150 Kč	0,75 Kč	0,5 Kč	0,25 Kč	0,5 Kč	1,5 Kč	0,5 Kč	0,25 Kč
Systém druhý	4,250 Kč	1,5 Kč	0,5 Kč	0,25 Kč	0,25 Kč	1 Kč	0,5 Kč	0,25 Kč
Systém třetí	15,000 Kč	1 Kč	0,5 Kč	0,25 Kč	1 Kč	0,5 Kč	0,25 Kč	0,25 Kč

Zdroj: vlastní

1.4 Kapitálové plánování[6] a funkčnost systému

Kapitálové plánování je dlouhodobý, trvalý a soustavná proces plánování, zajišťování kapitálových výdajů a peněžních toků související se záměrem, jehož teoretická návratnost je dlouhodobá. Základem pro výběr vhodných investic kapitálového plánování je investiční strategie, který vychází z projektu – záměru. Kvalitní a vhodná investice není možná bez zpracování různých variant projektů, zhodnocení rizik a způsobu financování. Rozhodnutí o investici je ovlivněna strategickým významem záměru, velikostí, rizikem, konkurencí a hlavně finančními nároky záměru.

1.4.1 Varianty rozhodování nutné pro posouzení projektu - záměru

- Vliv investice na konkurenční schopnost růstem užitnosti výrobku,
- Kritérium času investičního procesu,
- Vliv investice na kriterium kvantitativní stránky uspokojování poptávky po službě, výrobku,
- Vliv investice na realizovatelnost příslušného záměru
- Kriterium sociálních stránek služby umožněné záměrem
- Peněžní kritéria – efektivnost vynaložených zdrojů (hodnocení, varianty, zdroje, rizika)

[6] Prof. Ing. Konečný,M.,: „Finance podniku“, učební texty vysokých škol, VUT, fakulta podnikatelská, str. 18

Na základě analýzy současného stavu všech systémů a požadavků uživatelů je navržena nová systemizace uživatelů. Z analýzy vyplývá, že nový komunikační a informační systém musí umožňovat zpracovávání a přenos informací od stupně utajení „VYHRAZENÉ“ ve formě datových souborů, hlasových informací a foto-video sekvencí. Kapacita systému musí být modulová. Systém musí zajistit důvěrnost, integritu a dostupnost informací a to i v době nebezpečí a krizových situací.

Systém bude budován správy s využitím protokolu TCP/IP[7] s podporou VoIP (hlasová komunikace). Jednotlivá pracoviště informačního systému budou vybavena počítačovou sestavou a IP telefonem nebo LAN sítí. Pracoviště bude umožňovat zpracování citlivých informací prostřednictvím standardních kancelářských aplikací, odesílání a příjem citlivých informací (e-mail) a vedení utajených telefonních hovorů. K zajištění důvěrnosti a integrity přenášených utajovaných skutečností budou použity IP kryptografické prostředky certifikované NBÚ.

Tvorba architektury virtuálních sítí a jejich kontrola v rámci bezpečného komunikačního prostředí na úrovni IP protokolu, včetně přidělování klíčů k zajištění kryptografických funkcí, bude zajištěna z centrálního pracoviště. Pro implementaci hlasových služeb do prostředí IP bude sloužit centrální hlasový server, který bude komunikovat s potřebnými technologiemi v jednotlivých objektech. Součástí centrálního pracoviště bude i technologie pro podporu datových služeb (např. e-mail). Systém umožní další rozšiřování funkcí a služeb včetně propojování s jinými obdobnými systémy.

Komunikační a informační systémy musí splňovat podmínky, jelikož jsou schváleny a certifikovány NBÚ podle standardů NATO[7].

[7] Guide to Securing Microsoft Windows XP „ Operational Network Evaluations Division of the Systems and Network Attack center (SNAC)

Obrázek č.1: Systémové řešení bezpečnosti informačního systému

Zdroj: www.MVCR.cz

1.5 Finanční analýza a metody hodnocení investic

Metody finanční analýza rozdělujeme obecně na metody elementární a metody vyšší s dvěma typy ukazatelů a to extenzivní a intenzivní:

- **Extenzivní ukazatele** – charakterizují informace o rozsahu (objemu), představují kvantitu;
- **Intenzivní ukazatele** – charakterizují míru využití a jak rychle či silně se mění;[8]

1.5.1 Analýza stavových (absolutních) ukazatelů

- **Analýza trendů (horizontální analýza)** – porovnáváme změny ukazatelů v časové řadě. Informace lze získat v účetních výkazech a výročních zprávách za období delší než 5 let. Zdrojem jsou změny absolutních hodnot, i procentuální změny položek výkazu po řádcích tedy horizontálně.

[8] Kovanicová, D., Kovanic, P.,: Podklady skryté v účetnictví, díl II. D, Finanční analýza účetních výkazů, Praha. 199, str. 22

- **Procentní rozbor (vertikální analýza)** – porovnáváme změny ukazatelů majetku a kapitálu (strukturu aktiv a pasiv). Z rozboru lze odvodit složení prostředků potřebných pro výrobní a obchodní aktivity společnosti a z jakých zdrojů byly pořízeny. Vytvoření rovnovážného stavu a jeho udržení závisí na ekonomické stabilitě společnosti.[9]

1.5.2 Analýza rozdílových a tokových ukazatelů

- **Analýza fondů finančních prostředků** – jsou fondy finančních prostředků, které se nazývají rozdílové ukazatele sloužící k analýze a řízení finanční situace podniku s ohledem na likviditu. Tuto analýzu je nutno chápat jako agregaci stavových ukazatelů vyjadřující aktiva nebo pasiva v krátkodobém horizontu podle:
    - **Čistého pracovního kapitálu** – jedná se o rozdíl ∑ OA/∑ krátkodobých dluhů
    - **Čisté pohotové prostředky** – jedná se o rozdíl ∑ pohotových peněžních prostředků/∑ okamžitým splaceným závazkům
    - **Čisté peněžně pohledávkové finanční fondy** – jedná se o rozdílové ukazatele čistých fondů finančních prostředků za předpokladu, že společnost část OA financuje dlouhodobými cizími zdroji

1.5.3 Analýza Cash flow

CF – peněžní tok vyjadřuje skutečný pohyb peněžních prostředků firmy. Je jedním ze základních hledisek likvidity. Kde analýza je důsledně založena na příjmech a výdajích a vyjadřuje reálné toky peněz a jejich zásob ve společnosti. Výchozí datovou základnou pro analýzu CF[21] je účetnictví podniku, které důsledně informuje o tvorbě finančních zdrojů v čase a slouží k získání podrobných informací o finanční situaci ve společnosti podle následujících metod[10]:

[9] Kovanicová, D., Kovanic, P.,: Podklady skryté v účetnictví, díl II. D, Finanční analýza účetních výkazů, Praha. 199, str. 22
[10] Sedláček, J.,: Účetní data v rukou manažéra – finanční analýza v řízení firmy, Computer Press Praha, 2001 str. 51, 59

- **Metoda sledování skutečných příjmů a výdajů**
- **Transformace výnosové nákladových dat na příjmově nákladová**
- **Transformace hospodářského výsledku na Cash Flow**
- **Metody poměrových ukazatelů obsahující Cash Flow**

1.5.4 Analýza ukazatelů likvidity

Likvidita je typická charakteristika společnosti v kterýmkoliv okamžiku dostát svým závazkům, přeměnit majetek na peníze. Čím vyšší likvidita tím nebezpečnější platební neschopnost. Vyjadřující dluhy společnosti jsou větší než reálná hodnota aktiv. Základní ukazatele likvidity:

- Okamžitá likvidita = likvidita 1. stupně – vyjadřuje schopnost hradit právě splatné dluhy, hodnota okamžité likvidity by měla být v intervalu <0,2;0,6>

$$\text{Okamžitá likvidita} = \frac{\text{Finanční majetek}}{\text{okamžitě splatné závazky}}$$

- Rychlá (pohotová) likvidita = likvidita 2. stupně – odstraňuje nedostatky okamžité likvidity, hodnota rychlé likvidity by měla být v intervalu <1;1,5>,

$$\text{Rychlá likvidita} = \frac{\text{oběžní aktiva - zásoby}}{\text{krátkodobé závazky}}$$

- Běžná likvidita = likvidita 3. stupně – vyjadřuje kolik krát oběžní aktiva pokryjí krátkodobé závazky, hodnota běžné likvidity by měla být v intervalu <1,5; 3>,

$$\text{Běžná likvidita} = \frac{\text{oběžní aktiva}}{\text{krátkodobé závazky}}$$

1.5.5 Analýza ukazatelů rentability

- Analýza ukazatelů rentability – (ROI) ukazatel vyjadřuje s jakou účinností působí celkový kapitál vložený do firmy nezávisle na zdroji financování.

$$ROI = \frac{\text{zisk před zdaněním + nákladové úroky (EBIT)}}{\text{celkový kapitál}}$$

- Analýza ukazatelů aktivity – (ROA) ukazatel poměřuje zisk s celkovými aktivy investovanými do podnikání bez ohledu na to, z jakých zdrojů jsou financována.
    - Pokud **EBIT** je provozní zisk, potom měříme hrubou produkční sílu aktivit firmy před odečten daní a nákladových úroků.

$$ROA = \frac{\text{EBIT}}{\text{celkový aktiva}}$$

    - Pokud **„čistý zisk“** zvýšený o zdaněné úroky, ukazatel poměřuje vložené prostředky nejen se ziskem + úroky, jež jsou odměnou věřitelům za jejich zapůjčený kapitál

$$ROA = \frac{\text{čistý zisk před zdaněním}}{\text{celkový aktiva}}$$

- Analýza ukazatelů rentability VK – (ROE) ukazatel poměřuje míru ziskovosti VK, zda je dostatečně výnosný a zda je využíván s maximální intenzitou odpovídající investičnímu riziku. Podmínka pro ROE > úroky, které by společnost obdržela při jiné formě investování.

$$ROE = \frac{\text{čistý zisk}}{\text{VK}}$$

- Analýza ukazatelů rentability dlouhodobých zdrojů – (ROCE) ukazatel slouží k časoprostorovému srovnání firmy k hodnocení monopolních veřejně prospěšných společností.

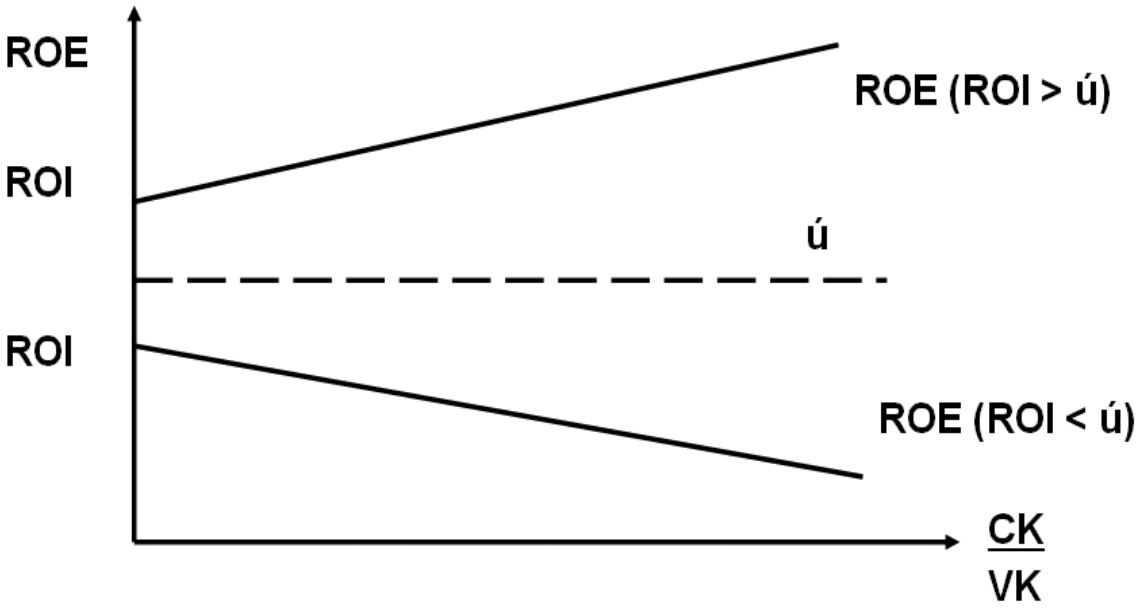
$$ROCE = \frac{\text{HV po zdanění + nákladové úroky}}{\text{dlouhodobé závazky + VK}}$$

- Finanční páka – je ukazatel poměru vlastního kapitálu k ziskovosti celkových kapitálu. Tento pojem je nutno chápat jako možnost zvýšení ziskovosti VK připojením cizích zdrojů k VK

$$\text{Finanční páka} = \frac{\text{Cizí kapitál + vlastní kapitál}}{\text{vlastní kapitál}}$$

Z analýzy poměrových ukazatelů lze odvodit následující vztah, pokud je úroková míra úplatných cizích zdrojů (náklady na cizí kapitál) nižší než ziskovost celkového úplatného kapitálu, roste ziskovost vlastního kapitálu při přílivu cizích zdrojů financování (jsou levnější). Je-li naopak ziskovost celkového úplatného kapitálu nižší než úroková míra úplatných cizích zdrojů financování, klesá s rostoucí zadlužeností ziskovosti vlastního kapitálu.

Obrázek č.2: Finanční páka – závislost ROE na úroku



Zdroj: vlastní

1.5.6 Analýza ukazatelů zadluženosti

Udává vztah mezi cizím a vlastním kapitálem[20] nebo jejich složkami. Ukazatele zadluženosti (debet management) vypovídají o tom, kolik majetku podniku je financováno cizím kapitálem. Tyto ukazatele zajímají především investory a poskytovatele dlouhodobých úvěrů.

- Celková zadluženost = „ukazatel věřitelského rizika“ – ukazatel poměřuje podíl cizího kapitálu k celkovým aktivům. Čím větší je podíl VK tím větší je bezpečí ztrát věřitelů v případě likvidity. Preference je nízká zadluženost pro věřitele, naopak vlastníci hledají cizí zdroje , aby znásobili a zvýšili výnosy. Hodnota by měla být stejná jako oborový průměr, pokud je vyšší, má firma problém získat nové zdroje a je nutné zvýšit VK.

$$\text{Celková zadluženost} = \frac{\text{cizí zdroje}}{\text{aktiva celkem}}$$

  - Koeficient samofinancování – ukazatel dává přehled o tom do jaké míry jsou aktiva financována VK

$$\text{Koeficient samofinancování} = \frac{\text{vlastní kapitál}}{\text{aktiva celkem}}$$

- Úrokové krytí – ukazatel informuje kolikrát převyšuje zisk placené úroky. Část zisku z CK by měla pokrýt náklady na vypůjčený kapitál. Hodnota by měla být v intervalu $<\infty;0,9>$, hodnota $<1>$ znamená, že na zaplacení úroků je třeba celého zisku.

$$\text{Úrokové krytí} = \frac{\text{EBIT}^{11}}{\text{nákladové úroky}}$$

  - Krytí fixních poplatků – ukazatel rozšiřuje předcházející ukazatel o stálé platby, hrazené pravidelně za použití cizího kapitálu (leasingové splátky)

$$\text{Krytí fixních poplatků} = \frac{\text{EBIT + dlouho. splátky}}{\text{nákladové úroky + dlouho. splátky}}$$

[11] EBIT (Earnings befor Interest and Texas) – zisk před úroky s daněmi

- Dlouhodobá zadluženost – ukazatel vyjadřuje jaká část firmy je financována dlouhodobými dluhy. Poměr dlouhodobých a krátkodobých cizích zdrojů.

$$\text{Dlouhodobá zadluženost} = \frac{\text{dlouhodobý cizí kapitál}}{\text{celková aktiva}}$$

$$\text{Běžná zadluženost} = \frac{\text{krátkodobý cizí kapitál}}{\text{celková aktiva}}$$

$$\text{Dlouhodobé krytí aktiv} = \frac{\text{VK + cizí kapitál}}{\text{celková aktiva}}$$

$$\text{Dlouhodobá zadluženost k vloženému kapitálu} = \frac{\text{dlouhodobý cizí kapitál}}{\text{základní kapitál}}$$

1.5.7 Analýza ukazatelů aktivity

Schopnost společnosti jak efektivně vynakládat se svými aktivy. Čím více aktiv, než je nutné pro chod společnosti, tím vyšší nepotřebné náklady a naopak. Standardní ukazatele aktivity:

- Obrat celkových aktiv – ukazatel vyjadřuje, zda pořídit další produkční investiční majetek. Hodnota by měla být vyšší než oborový průměr, pokud je nižší (chybí slovo) zvýšit výrobu a omezit investice.

$$\text{Obrat stálých aktiv} = \frac{\text{roční tržby}}{\text{stálá aktiva}}$$

- Obrat zásob – ukazatel vyjadřuje intenzitu využití zásob a udává, kolikrát v roce je každá položka zásob prodaná a znovu naskladněná. Hodnota by měla být stejná jako oborový průměr, pokud je vyšší má firma zbytečné zásoby vyžadující nadbytečné financování.

$$\text{Obrat zásob} = \frac{\text{roční tržby}}{\text{zásoby}}$$

- Doba obratu zásob – ukazatel vyjadřuje průměrný počet dnů, po které jsou zásoby vázány v podnikání do doby jejich spotřeby nebo prodeje. U zásob výrobků a zboží je ukazatelem likvidity

$$\text{Doba obratu zásob} = \frac{\text{průměrné zásoby}}{\text{denní tržby}}$$

- Doba obratu pohledávek – ukazatel vyjadřuje poměr stavu pohledávek k průměrným denním tržbám na obchodní úvěr

$$\text{Doba obratu pohledávek} = \frac{\text{obchodní pohledávky}}{\text{denní tržby na fakturu}}$$

- Doba obratu závazků – ukazatel vyjadřuje poměr stavu závazků k průměrným denním tržbám na obchodní úvěr

$$\text{Doba obratu závazků} = \frac{\text{obchodní závazky}}{\text{denní tržby na fakturu}}$$

1.5.8 Analýza soustav ukazatelů

- Rychlý test (Quick test) – poskytuje rychlou odpověď s poměrně velmi dobrou vypovídací schopností analyzovat firmu. Používá se čtyř oblastí po jednom ukazateli, které nesmí podléhat rušivým vlivů a musí vyčerpávajícím způsobem reprezentovat celý informační potenciál rozvahy a výkazu zisku a ztrát.

    - Kvóta vlastního kapitálu – ukazatel charakterizuje dlouhodobou stabilitu a samostatnost, určuje míru potřeby pokrytí své potřeby vlastními zdroji, při zjištění poklesu rentability[12]

$$\text{Kvóta vlastního kapitálu} = \frac{\text{vlastní kapitál}}{\text{celková aktiva}}$$

    - Doba splacení dluhu – ukazatel charakterizuje za jaké časové období je podnik schopen uhradit své závazky. Bilanční Cash Flow získáme odečtením daně z příjmu a odpisů HM + NHM od HV.

$$\text{Doba splácení dluhu} = \frac{\text{cizí kapitál} - \text{likvidní prostředky}}{\text{bilanční Cash Flow}}$$

[12] Sedláček, J.,: Účetní data v rukou manažéra – finanční analýza v řízení firmy, Computer Press Praha, 2001 str. 124

- Cash Flow v % tržeb – ukazatel charakterizuje spolu s kvótou VK finanční stabilitu a její recipročí hodnotu jako solventnost dané firmy.

$$\text{Cash Flow v \% tržeb} = \frac{\text{provozní Cash Flow}}{\text{celková aktiva}}$$

- Rentabilita celkového kapitálu – (ROA) ukazatel analyzuje výnosovou situaci zkoumané firmy.

$$\text{Rentabilita celkového kapitálu} = \frac{\text{HV po zdanění + úroky (1. daň. sazba)}}{\text{celková aktiva}}$$

Bonita společnosti se stanoví tak, že každý ukazatel se podle dosaženého výsledku nejprve oklasifikuje, vloží se do tabulky a výsledná hodnota se určí aritmetickým průměrem hodnot za jednotlivé ukazatele, totéž je vhodné vypočítat pro finanční stabilitu a výnosovou situaci.

Tabulka č.7: Bonita společnosti podle ukazatelů

Ukazatel	Výborný [1]	Velmi dobrý[2]	Dobrý[3]	Špatný[4]	Ohrožen insolvencí[5]
Kvóta VK	> 30%	> 20%	> 10%	>0%	negativní
Doba splácení dluhu	< 3 roky	< 5 let	< 12 let	> 12 let	> 30 let
CF v % tržeb	> 10%	> 8%	> 5%	>0%	negativní
ROA	> 15%	> 12%	> 8%	>0%	negativní

Zdroj: Sedláček, J.,: Účetní data v rukou manažera – finanční analýza v řízení firmy, Computer Press Praha, 2001 str. 125

- Altmanův index finančního zdraví (Atmanovo Z-skóre) – poskytuje prognózu finanční situace společnosti, vychází matematicko-statistické diskriminační vícerozměrné analýzy,

$$Z = 0{,}717 * \frac{ČPK}{A} + 0{,}847 * \frac{ner.HV\ \min .obd}{A} + 3{,}107 * \frac{EBIT}{A} + 0{,}42 + \frac{ZK}{CZ} + \frac{Tržby}{A}$$

ČPK	čistý pracovní kapitál
A	aktiva
ZK	základní kapitál
CZ	cizí zdroje

- Index IN 01 – poskytuje výsledky empiricko-induktivních ukazatelových systémů, ratingu a praktické zkušenosti při analýze finančního zdraví podniku.

$$IN01 = 0{,}13 * \frac{A}{CZ} + 0{,}04 * \frac{EBIT}{Ú} + 3{,}92 * \frac{EBIT}{A} + 0{,}21 * \frac{VYN}{A} + 0{,}09 * \frac{KZ}{KBU}$$

VYN	výnosy
KBU	krátkodobé bank. Úvěry

- Ekonomická přidaná hodnota – model EVA poskytuje informace na ekonomickém zisku, jako rozdíl účetního zisku představuje přebytek výnosů, zůstávající firmě po zaplacení služeb výrobních faktorů nejen cizího i vlastního kapitálu. Jedná se o hodnotu, přidanou vlastní činností firmy nad úroveň vložených nákladů. Hodnota EVA > 0 vytváří hodnotu pro vlastníky.

$$EVA = NOPAT - WACC * C$$

$$WACC = r_d * \frac{D}{C} * (1 - t) + r_e * \frac{E}{C}$$

NOPAD	čistý provoz. zisk za sled. období
WACC	vážený průměr nákladů na kapitál
D	cizí úplatný kapitál
E	vlastní úplatný kapitál
C	celkový investovaný kapitál
r_d	úroková míra p.s. cizího kapitálu
r_e	požadovaná výnosnost VK
t	míra daně z příjmů PO

- Du Pontův rozklad
- Pyramidové rozklady

1.5.9 Metody hodnocení efektivnosti investičních

1.5.9.1 Zohlednění podle faktor času – metody statické, dynamické

1.5.9.2 Zohlednění podle efektů z investičního projektu

- metoda založená na úspoře investičních výdajů a provozních nákladů
- metoda založená na zisku po zdanění
- metoda založená na peněžním toku (Cash – flow)

1.5.9.3 Metoda „Čisté současné hodnoty“projektu – [Net Present Value of Investment **“** – NPV] – projekt je možno přijmou pokud hodnota je větší než „0“,

1.5.9.4 Metoda „Vnitřní míry výnosu“ – [Internal Rate of Retung – IRR] – projekt je možno přijmou pokud hodnota je větší než „0“,

1.5.9.5 Metoda „Míry výnosu“ – bez faktoru času

$$\bar{r}_l = (P - K) m / K$$

s faktorem času

$$\bar{r}_l = (SHP - SHK) m / SHK$$

při seriózním posouzení se používá „míra výnosu“ s faktorem času,

1.5.9.6 Metoda „Doby splácení“ – [Payback Method] – období, za které „peněžní tok příjmů“ přinese hodnotu rovnající se „kap. výdajům“ čím je doba kratší, tím je výhodnější projekt – záměr,

1.5.9.7 Metoda „Koeficientu efektivnosti dodatkových kap. výdajů – pracuje s údaji dvou investičních variant, kdy první má nižší kap. výdaje na investici[K], ale vyšší průměrné provoz. náklady [Ñ] než druhá varianta,

$$k_{ef} = \left(\bar{N}_1 - \bar{N}_2 \right) / (K_1 - K_2)$$

varianta s vyššími kapitálovými výdaji je výhodnější,

1.5.9.8 Metody „Průměrných ročních převedených nákladů“ – používá se bez faktoru času,

$$\overline{PRN} = Ñ + k*K$$

varianta s nejnižšími průměrnými ročními „převedenými náklady“ je nejvýhodnější

1.5.10 Ukazatele tržní hodnoty

Je schopnost společnosti, jako podnikatelského subjektu o proniknutí na trhy v minulém sledovaném období a vývoj trendů. Standardní ukazatele tržní hodnoty jsou:

- Price/earning Ration = cena akcie/zisk na jednu akcii;
- Market/Book Ration = tržní cena akcie/nominální hodnota akcie;

2 Charakteristika společnosti

2.1 Obecný popis společnosti

Uvedená společnost jako podnikatelský subjekt je na trhu od roku 1991. Pro úspěšné podnikání, financování a zpracování jednotlivých zakázek je nutné vypracovat podnikatelský záměr[3], který charakterizuje a upřesňuje odpovědnost a financování, analyzuje, kontroluje a stanovuje cíle záměru. Všechny tyto jednotlivé na sobe navazující činnosti vedou k dosažení úspěšného splněné podnikatelského záměru a tudíž i maximalizují jeho zisk jako základní produkt podnikání. Společnost, která vypracovává podnikatelský záměr na bezpečný komunikační a informační systém on-line pro státní správu je společnost „**TELE**fonní a ko**MU**nikační **Z**ařízení“ dále jen **„TELEMUZ s.r.o.“**, se sídlem: Selská 141, 613 00 Brno-Maloměřice.

Společnost s ručením omezeným (dále s.r.o.) je kapitálovou společností. Tato forma patří k nejběžnějším formám obchodních společností v České republice. Výhodou oproti ostatním společnostem je to, že se u této formy podnikání skládá poměrně malý základní kapitál.

Společnost pak ručí svým majetkem a společníci pouze do výše svých vkladů. Nevýhodou se může zdát, že firmy zapsané v obchodním rejstříku musí vést účetnictví, ne daňovou evidenci. Nevýhodou pro společníky je zákaz konkurence.

Uvedená společnost „TELEMUZ s.r.o.“ byla založena fyzickými společníky, kteří podnikají na základě živnostenského oprávnění vydaného Živnostenským úřadem v Brně v roce 1991. Vlastní podnikání se řídí ustanovením Obchodního zákoníku č. 513/1991 Sb. pro právnické osoby ve znění pozdějších novel. Firma je plátcem DPH - DIČ 123-87654321 (FÚ Brno II).

Společnost je zapsána v Obchodním rejstříku vedeném Krajským obchodním soudem v Brně, oddíl C vložka 9876. Oba vlastníci jsou zároveň jednatelé společnosti a mají právo za společnost zastupovat a podepisovat smlouvy jednotlivě. Každý ze společníků firmy podepsal společenskou smlouvu, kterou mezi sebou sepsali, mající poloviční podíl na čistém zisku. Společnost má v současné době 45 zaměstnanců (viz

organizační schéma str. 24, rozděleni do několika divizí. Oba spoluvlastníci jsou zároveň zaměstnanci společnosti.

Společnost „TELEMUZ s.r.o.“ je plátcem DPH. Toto rozhodnutí být plátcem je podmíněno skutečností, že většina subdodavatelů společnosti jsou plátci DPH. Zisk vyprodukovaný kapitálovou společností - s.r.o je zdaněn ve dvou stupních:

- U společnosti – dani z příjmů právnických osob (DPPO);
- U společníků – jako podíl zisku v našem případě daní z příjmu fyzických osob (DPFO);

V tomto zdaňování se s.r.o. žádným způsobem neodlišuje od akciové společnosti či družstva, přesto odměna vyplácená jednateli s.r.o. je daňovým nákladem s.r.o., zatímco obdobné odměny vyplácené členům předsednictva a.s. či družstva jsou nedaňovým nákladem.

Tabulka č.4: Identifikace prvního společníka společnosti „TELEMUZ s.r.o.“

Titul, jméno, příjmení	Ing. Boris Treblík	
Datum narození	21.1.1960	okres Brno – město
Rodinný stav	Ženatý	
Bydliště	Husova 577, Modřice u Brna	602 00 Brno
Vzdělání	VUT Brno – fakulta elektrotechniky a komunikačních technologii, VŠZ – fakulta ekonomiky	

Zdroj: společnost „TELEMUZ s.r.o.“

Tabulka č.5: Identifikace druhého společníka společnosti „TELEMUZ s.r.o.“

Titul, jméno, příjmení	Ing. Zdeněk Svoboda	
Datum narození	9.1.1959	okres Brno – město
Rodinný stav	Rozvedený	
Bydliště	Nad tratí 131, Bílovice nad Svitavou	Brno – venkov
Vzdělání	VUT Brno – fakulta elektrotechniky a komunikačních technologii	

Zdroj: společnost „TELEMUZ s.r.o.“

Tabulka č.6: Všeobecné informace o společnosti „TELEMUZ s.r.o.“

Právní forma podniku	Společnost s ručením omezením
Používaná zkratka	s.r.o.
Sídlo společnosti	Selská 141, 613 00 Brno-Maloměřice
Provozovna společnosti	Selská 141, 613 00 Brno-Maloměřice
Bankovní spojení	
BÚ u Československé obchodní banky (ČSOB)	Křenová 25, 602 00 Brno
Číslo běžného účtu	3142277389/0300
Adresa ČSOB	Šumavská 33, 611 40 Brno

Zdroj: společnost „TELEMUZ s.r.o.“

2.2 Předmět činnosti společnosti „TELEMUZ s.r.o.“

Předmět podnikání byl zvolen s ohledem na vzdělání majitelů společnosti, kdy oba získali vysokoškolské vzdělání v oboru elektrotechniky a komunikačních technologii. V tomto oboru pracovali ve státní správě, kde získaly praktické zkušenosti, které doplňovali získanými teoretickými znalostmi ze školy. Ve státní správě oba poprvé získali kontakt s komunikačními a informačními systémy na přenos videa a zvuku a s prvními informačními systémy pracující s PC na lokální bázi zpracovávající utajované a citlivé skutečnosti.

V roce 1990 oba odešli od státní správy a jejich původní podnikatelský záměr se obracel na malé a střední podnikatele, státní správu, ale i na občany, poskytující těmto subjektům služby v oblasti telekomunikačních, zabezpečovacích a informačních systémů. Společnost poskytovala služby v rozsahu výstavby novou progresivní technikou od firem Siemens, Alcatel, DSC a jiných renovovaných firem. Management společnosti vytvořil smlouvy na záruční a pozáruční servis on-line s maximální dobou opravy do 48 hodin. V té době to byl strategicko-manažerský tah, který společnosti velice pomohl k novým zákazníkům, a tím i splnit podnikatelský záměr maximalizovat zisk[10], [21] z podnikání.

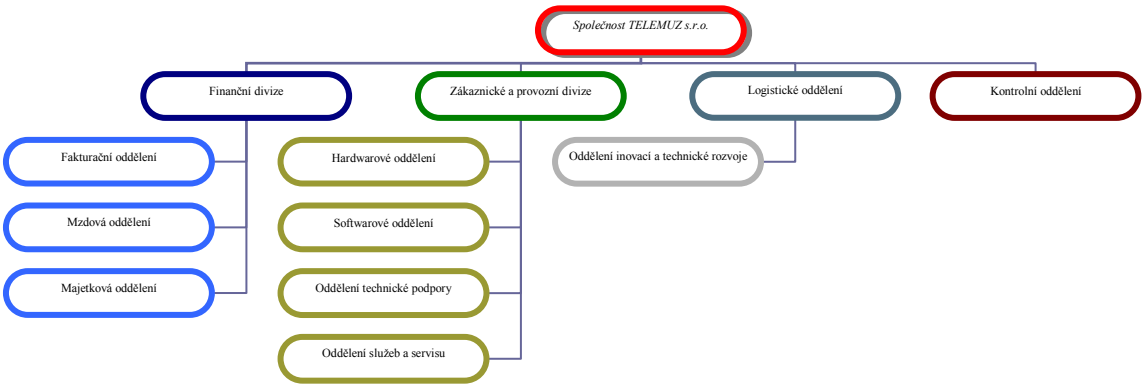
Společnost spolupracuje s odborníky, kteří pro klienty společnosti navrhují opatření v rámci vědeckého-technického rozvoje v oblasti telekomunikačních, zabezpečovacích a informačních systémů.

Společnost „TELEMUZ s.r.o.“ si v roce 1999 požádala NBÚ o povolení k přístupu k utajovaným skutečnostem do stupně utajení „DŮVĚRNÉ“, jelikož začala spolupracovat s orgány státní správy. V roce 2000 NBÚ vydal společnosti certifikát „O ochraně utajovanými skutečnostmi“ do stupně „DŮVĚRNÉ“ podle zákona č. 148/1998 Sb.

Od ledna 2005 platí nový zákon č. 412/2005 Sb., „O ochraně utajovaných informací a personální bezpečnosti“[30], včetně vyhlášek NBÚ[37], [38, [39], [40], [41] a proto společnost zažádala o prodloužení certifikátu a začala se zabývat teoretickou přípravou komunikačních a informačních systémů pro ochranu utajovaných informací a dat, včetně zálohování pomocí počítačových komponentů a sítě. Vzhledem k této skutečnosti požádala sekci NBÚ zabývající se bezpečností počítačových sítí o vypracování bezpečnostní posudku na bezpečnostní politiky pro vlastní informační systém, který by mohl sloužit jako základ pro ostatní systémy, které společnost hodlá v rámci podnikatelského záměru nabízet na trhu.

Navrhovaný komunikační a informační systém musí splňovat všechny požadavky pro ochranu utajovaných a citlivých informací o klientech, projektech a investicích, stavu a finančních operacích společnosti, zamezit nekompetentním osobám přístupu k těmto informacím a datům, zajistit bezpečné nakládání s informací důležitých pro společnost a případně stanovit obnovu systému pokud dojde k poškození nebo totálnímu kolapsu.

Obrázek č.3: Organizační schéma společnosti „TELEMUZ s.r.o.“



Zdroj: společnost „TELEMUZ s.r.o.“

2.3 Kapitál a majetek společnosti

Jedná se o základní strukturované komodity[18], [21] potřebné k podnikání, které mají charakter hmotných či nehmotných prostředků, vlastního či cizího kapitálu. Jmenované prostředky se během podnikání v závislosti na riziku, čase, okolních vlivech mění a jejich stavy lze sledovat v rozvaze společnosti, jelikož je to jeden ze základních dokumentu, který je tvořen na začátku a konci účetního období.

Tabulka č.6: Všeobecná struktura výkazu zisku a ztrát (výsledovky)

A. PRODEJNÍ (OBCHODNÍ) ČINNOST
Tržby za prodané zboží
- Náklady na prodané zboží
= OBCHODNÍ MARŽE
B. VÝROBNÍ ČINNOST
Tržby z prodeje výrobků
- výrobní spotřeba
= rozdíl + OBCHODNÍ MARŽE = PŘIDANÁ HODNOTA
- Osobní náklady
- Daně, poplatky a jiné náklady
- Odpisy hmotného a nehmotného investičního majetku
= PROVOZNÍ HOSPODÁŘSKÝ VÝSLEDEK
C. FINANČNÍ ČINNOST
Finanční výnosy
- Finanční náklady
= HOSPODÁŘSKÝ VÝSLEDEK Z FINANČNÍCH OPERACÍ
CELKEM
hospodářský výsledek B a C
- Daň z příjmů
= HOSPODÁŘSKÝ VÝSLEDEK Z BĚŽNÉ ČINNOSTI
D. MIMOŘÁDNÁ ČINNOST
Mimořádné výnosy
- Daň z příjmů z mimořádné činnosti
= MIMOŘÁDNÝ HOSPODŘÁSKÝ VÝSLEDEK
CELKEM hospodářský výsledek C a D = HOSPODÁŘSKÝ VÝSLEDEK ZA ÚČETNÍ OBDOBÍ

Zdroj: vlastní

2.4 Úloha financí ve společnosti „TELEMUZ s.r.o.“

Každý podnikatelský záměr[3] musí být podpořen, kryt a realizován z podnikových financí, které se na daný podnikatelský záměr musí shromáždit, buď z vlastních nebo cizích zdrojů. Je nutné, aby každý záměr byl na podroben finanční analýze s následným vyhodnocením a konkrétním rozhodnutím, zda záměr přijmout či zamítnout podle následujících parametrů: Finanční analýzu lze shrnout do tří vzájemně propojených úkolů:

1. Ke zjišťování pozitivních a negativních trendů dopadů na firmu, poskytující zpětnou vazbu o naplňování strategických cílů při rozhodování managementu. Zjišťování trendů v časové rovině minulého a budoucího vývoje s důrazem na budoucnost s poučením se z chyb minulosti;
2. odhalit příčiny negativního či pozitivního vývoje, neboť samotný výpočet ukazatelů nabízí pouze jeho matematickou interpretaci;
3. stanovit aktivity, priority, které podpoří pozitivní a dynamický vývoj a změní negativní výsledky[13]

Podnikové finance se zabývají rozdělením toků mezi jednotlivé zájmové skupiny důležité pro společnosti jako jsou: dodavatelé, bankovní instituce, zákazníci, vlastnícj, veřejnoprávní instituce a vlastní zaměstnanci.

Úlohou řízení podnikových financí[21] je zajištění dostatečného likvidního množství financí pro všechny aktivity společnosti a jejich agresivních tak obranných opatření na konkurenčním trhu v následujících oblastech:

- řízení aktiv – rozhodování o investicích,
- řízení pasiv – rozhodování o zdrojích investování,
- řízení informací – podpůrná a dokumentační funkce,
- řízení rizik – identifikování, ohodnocení, opatření na řešení,

K řízení podnikových financí slouží také finanční analýza jakožto matematicko analytický nástroj podnikání s úzkou vazbou na finanční zdroje, kriticky a s vysokou pravděpodobností lze vyhodnotit úspěšnost podnikání, podnikatelských záměrů a

[13] Vosoba, P,. Řízení firemních aktivit – aktivní využití finančních zdrojů, Praha, str. 164

rozhodnutí managementu o dalších aktivitách, jako jsou půjčky, úvěry, leasingy od bankovních institucí na další rozvoj společnosti.

Finanční analýza[21] disponuje celou řadou metod, které svými výpočty podporují řadu rozhodnutí managementu o dalším vhodném vývoji a řešení financování podniku ve všech oblastech podnikání.

2.5 Konkurenční výhoda projektu

Každá firma na současném konkurenčním trhu[23] realizuje svoje výrobky a služby za účelem maximalizovat zisk, získat konkurenční výhodu, ovládnout (monopolizovat) trh. Pro tuto činnost musí mít management společnosti promyšlené dlouhodobé strategické cíle s přesně vymezenými a definovanými výhodami a službami pro potencionální zákazníky. Strategický, taktický i operativní cíl společnosti se musí rozvíjet intenzivně, explicitně, plánovitě, implicitně prostřednictvím aktivit společnosti v rámci právních a etických norem společnosti.

V každém časovém okamžiku světa, společnosti, ekonomice dochází ke konkurenčním střetům a výhodám nad ostatními konkurenty, kteří se taktéž maximálně snaží o konkurenční výhodu pro svoji firmu. Součástí konkurenční výhody je dlouhodobá činnost managementu ve všech oblastech činnosti společnosti jak ekonomické, personální, vzdělávací, podnikatelské, etické i normo-tvorné. Všechny tyto vlastnosti lze shrnout do oblasti speciálních managementů, které všechny vstupy maximalizují na výstupy pro uvedenou společnost.

Tabulka č.8: Přehled speciálních managementů společnosti

SPECIÁLNÍ MANAGEMENTY		
Management změny	Organizační management	Procesní management
Marketingový management	Strategický management	Logistický management
Management jakosti	Projektový management	Personální management

Zdroj: HODNOTOVÝ MANAGEMENT, doc. Ing. František Bartes, CSc., str. 3

3 Vlastní řešení podnikatelského záměru

Vlastní řešení podnikatelského záměru[20] vychází ze standardů NBÚ a standardů EU, včetně doporučení NATO. Základním požadavkem na nový moderní, robustní komunikační a informační systém je podpořit strategické, bezpečnostní, informační cíle státní správy, ochrana citlivých a utajovaných informací důležitých pro rozhodování a řízení na dobu, kdy je nutné získat konkurenční výhodu. Dosažením cíle je nutné sjednocení hardwarové, softwarové platformy s moderním nadčasovým kryptografickým prostředkem, který je srdcem a duší vlastní ochrany a v součinnosti s dalšími bezpečnostními prvky tvoří ucelenou bezpečnostní správu komunikačního a informačního systému.

Vlastní řešení systému zahrnuje kromě nákladů finančních, controllingových, logistických, bezpečnostních, zálohovacích, náklady na lidské zdroje, jejich vzdělanost, loajálnost, změnu kolektivu, ale i řídící a manažerské funkce a role.

Při vlastním řešení je nutné vycházet z detailního zadání podnikatelského záměru, z finančních možností organizace, z lidského potenciálu a výše rizik na ochranu dat a informací. Při řešení lze aplikovat bezpečnostní politiku na systém v několika přístupech:

- **Paranoidní** – absolutně vše zabezpečeno, vše je uživatelům zakázáno, vše se monitoruje, z důvodu bezpečnosti neexistuje výstup na periferní zařízení;
- **Přísná** – vše co není výslovně nebo písemně povoleno je zakázáno;
- **Povolná** – vše co není výslovně nebo písemně zakázáno je povoleno;
- **Promiskuitní** – vše je dovoleno, tedy i to, co by mělo být zakázáno z důvodu základní bezpečnosti;

Z předcházejícího odstavce je nutné konstatovat, že **první případ** znemožňuje práci v systému a takový systém nebude funkční pro bezpečnost dat a informací, uživatelé budou hledat vlastní nezabezpečená řešení pro zpracování dat a informací a vystavují organizaci riziku negativních dopadů. **Poslední případ** umožní práci v systému bez bezpečnostní politiky, neumožňuje a nezaručuje kontrolu nad zpracovávanými daty a informacemi, včetně jejich zcizení, poškození, nebo zničení.

Moje řešení podnikatelského návrhu je realizace bezpečného komunikačního a informačního systému pomocí všech schválených standardů NBÚ, NATO, EU. Použiji analýzy a metriky na všechny dostupné komponenty, ať hmotné či nehmotné, ale i na lidský potenciál jako hlavní zdroj hrozby, kompromitace, modifikace, destrukce, zneužití, interpretace a úniku chráněného zájmu.

Bezpečnostní politika a její nástroje si svými opatřeními musí chránit komunikační a informační systém jako aktivum za všech okolností proti vnějšímu i vnitřnímu nebezpečí. Musí být zpracovány plány mimořádných opatření, plány znovu obnovy systému při totálním kolapsu, systém zálohování, systém controllingu a vyhodnocování.

Vnějším nepřítelem lze nazvat neovlivnitelné přírodní jevy, dále poruchy techniky, proti kterým lze vytvořit standardní ochranné opatření, jako jsou objektové podmínky, pravidelné servisní zásahy, propracovaný zálohovací a obnovovací systém s následným testováním. Dalším nebezpečným vnějším nepřítelem je konkurence, terorismus ve všech formách projevu, který se systematicky a „hrubou silou“ snaží informace a data získat, nebo poškodit systém pomocí virů a škůdců.

Vnitřním nepřítelem lze nazvat vlastní pracovníky, které lze rozdělit do několika kategorií, a to na servisní pracovníky, kteří mohou nekontrolovaně, neomezeně a někdy i poškozovat, infiltrovat systém a na uživatele, kteří se snaží získat více práv nad systémem, než jim byla přidělena. Ve většině případů uživatel toto činí s úmyslem lépe, rychleji a efektivně pracovat.

I zde by bezpečnostní politika bezpečnostního systému měla zajistit standardní ochranu systému. Vnitřní nepřítel, který chce poškodit nebo zničit systém vždy přistupuje k systému úmyslně s cílem poškodit, zničit, infiltrovat či odcizit informace či data, pro získání vyšších přístupových práv než je mu systémem dáno.

3.1 Analýza hospodaření firmy „TELEMUZ s.r.o.“ za roky 2006 - 2008

V předcházející kapitole byly popsány teoretické nástroje analýzy firmy, které slouží k posouzení dlouhodobé maximalizaci tržní hodnoty podniku tzv. růst bohatství podnikatele. Rozhodujícími cíly je posouzení trvalé platební schopnosti podniku, trvalý dostatečně vysoký hospodářský výsledek a rentabilita vlastního kapitálu, jako podkladů pro bankovní společnosti, které poskytují zdroje financování podnikatelských záměru.

3.1.1 Analýza aktivit společnosti

Tabulka č.9: Analýzy horizontálních aktivit společnosti

Údaje jsou Kč, respektivě v %	2006	2007	2008	2007 - 2006	%	2008 - 2007	%
Aktiva celkem	**2 031 000**	**2 369 000**	**2 412 000**	**338 000**	**16,64%**	**43 000**	**1,82%**
Stálá aktiva	**27 000**	**0**	**394 000**	**-27 000**	**-100,00%**	**394 000**	**#DIV/0!**
DNM	0	0	0	**0**	**#DIV/0!**	**0**	**#DIV/0!**
DHM	27 000	0	394 000	**-27 000**	**-100,00%**	**394 000**	**#DIV/0!**
Dlouhodobý finanční majetek	0	0	0	**0**	**#DIV/0!**	**0**	**#DIV/0!**
Oběžná aktiva	**1 807 000**	**2 273 000**	**1 997 000**	**466 000**	**25,79%**	**-276 000**	**-12,14%**
Zásoby	408 000	432 000	538 000	**24 000**	**5,88%**	**106 000**	**24,54%**
Materiál	225 000	323 000	348 000	**98 000**	**43,56%**	**25 000**	**7,74%**
Nedokončená výroba	183 000	109 000	190 000	**-74 000**	**-40,44%**	**81 000**	**74,31%**
Výrobky	0	0	0	**0**	**#DIV/0!**	**0**	**#DIV/0!**
Zboží	0	0	0	**0**	**#DIV/0!**	**0**	**#DIV/0!**
Dlouhodobé pohledávky	**0**	**0**	**0**	**0**	**#DIV/0!**	**0**	**#DIV/0!**
Pohledávky z obchodního styku	0	0	0	**0**	**#DIV/0!**	**0**	**#DIV/0!**
Krátkodobé pohledávky	**1 250 000**	**1 727 000**	**1 301 000**	**477 000**	**38,16%**	**-426 000**	**-24,67%**
Pohledávky z obchodního styku	1 240 000	1 716 000	1 290 000	**476 000**	**38,39%**	**-426 000**	**-24,83%**
Krátkodobé poskytnuté zálohy	10 000	11 000	11 000	**1 000**	**10,00%**	**0**	**0,00%**
Krátkodobé finanční majetek	**149 000**	**114 000**	**158 000**	**-35 000**	**-23,49%**	**44 000**	**38,60%**
Peníze	19 000	79 000	13 000	**60 000**	**315,79%**	**-66 000**	**-83,54%**
Účty v bankách	130 000	35 000	145 000	**-95 000**	**-73,08%**	**110 000**	**314,29%**
Ostatní aktiva	**197 000**	**96 000**	**21 000**	**-101 000**	**-51,27%**	**-75 000**	**-78,13%**

Zdroj: společnost „TELEMUZ s.r.o.“

Podle rozložení majetku firmy, lze říci, že zvolený předmět podnikání se řadí mezi kapitálově méně náročné, jako ostatně většina služeb či obchodních aktivit.

Při rozboru jednotlivých položek oběžných aktiv, lze vysledovat zvýšený podíl zásob, který oproti minulým obdobím v roce 2006 vstoupl o cca 20%.

Dále můžeme pozorovat vysoký podíl krátkodobých pohledávek na celkovém majetku firmy, což si lze vysvětlit zhoršenou platební schopností odběratelů, která se projevuje v celé ekonomice společnosti. Druhotná platební neschopnost odběratelů se odráží i na značně se vykyvujícím krátkodobém finančním majetku (rozdíl až 315%).

Tabulka č.10: Analýzy vertikálních aktivit společnosti

Údaje jsou Kč, respektivě v %	2006	2007	2008	2006	2007	2008
Aktiva celkem	**2 031 000**	**2 369 000**	**2 412 000**	**100%**	**100%**	**100%**
Stálá aktiva	**27 000**	**0**	**394 000**	**1,33%**	**0,00%**	**16,33%**
DNM	0	0		0,00%	0,00%	0,00%
DHM	27 000	0	394 000	1,33%	0,00%	16,33%
Dlouhodobý finanční majetek	0	0	0	0,00%	0,00%	0,00%
Oběžná aktiva	**1 807 000**	**2 273 000**	**1 997 000**	**89%**	**96%**	**83%**
Zásoby	408 000	432 000	538 000	20%	18%	22%
Materiál	225 000	323 000	348 000	11,08%	13,63%	14,43%
Nedokončená výroba	183 000	109 000	190 000	9,01%	4,60%	7,88%
Výrobky	0	0	0	0,00%	0,00%	0,00%
Zboží	0	0	0	0,00%	0,00%	0,00%
Dlouhodobé pohledávky	**0**	**0**	**0**	**0,00%**	**0,00%**	**0,00%**
Pohledávky z obchodního styku	0	0	0	0,00%	0,00%	0,00%
Krátkodobé pohledávky	**1 250 000**	**1 727 000**	**1 301 000**	**61,55%**	**72,90%**	**53,94%**
Pohledávky z obchodního styku	1 240 000	1 716 000	1 290 000	61,05%	72,44%	53,48%
Krátkodobé pokynuté zálohy	10 000	11 000	11 000	0,49%	0,46%	0,46%
Krátkodobé finanční majetek	**149 000**	**114 000**	**158 000**	**7,34%**	**4,81%**	**6,55%**
Peníze	19 000	79 000	13 000	0,94%	3,33%	0,54%
Účty v bankách	130 000	35 000	145 000	6,40%	1,48%	6,01%
Ostatní aktiva	**197 000**	**96 000**	**21 000**	**9,70%**	**4,05%**	**0,87%**

Zdroj: společnost „TELEMUZ s.r.o.“

Z analýzy zdrojů financování firemního majetku vyplývá, že v roce 2006 a 2008 cizí zdroje značně převyšují vlastní kapitál (cca 5:1). Na tvorbě cizích zdrojů se podílejí krátkodobé závazky, které vznikají druhotnou platební neschopností firmy.

Na druhé straně však platí, že vlastní kapitál je drahým zdrojem financování a je tedy ekonomicky přínosné firmy do jisté míry zadlužit. Pokud se zastavíme u složení vlastních zdrojů, můžeme konstatovat, že jeho podstatnou složkou jsou nakumulované složky z minulých období, které zaznamenávají pozitivní rostoucí trend.

Negativně působí pokles hospodářského výsledku běžného období, který v roce 2007 razantně poklesl o 50%. V roce 2008 však tento ukazatel nabral opět pozitivní vývoj.

Co se týče cizích zdrojů financování můžeme říci, že se jejich podíl na celkových pasivech zvýšil ve sledovaném tříletém období o cca 25%.

3.1.2 Analýza tokových a rozdílových ukazatelů společnosti

Tabulka č.11: Analýzy tokových a rozdílových ukazatelů společnosti

Údaje jsou v tisících Kč, respektivě v %	2006	2007	2008	2007 - 2006	%	2008 - 2007	%
Pasiva celkem	2 031 000	2 369 000	2 412 000	**338 000**	**16,64%**	**43 000**	**1,82%**
Vlastní kapitál	-368 000	-500 000	-653 000	**-132 000**	**35,87%**	**-153 000**	**30,60%**
Základní kapitál	100 000	100 000	100 000	**0**	**0,00%**	**0**	**0,00%**
Kapitálové fondy	0	0	0	**0**	**#DIV/0!**	**0**	**#DIV/0!**
Reservní fondy	10 000	10 000	10 000	**0**	**0,00%**	**0**	**0,00%**
Výsledky hospodaření minulých let	-190 000	-492 000	-620 000	**-302 000**	**158,95%**	**-128 000**	**26,02%**
Výsledek hosp. běž. účet. obd. po zdanění	-288 000	-118 000	-143 000	**170 000**	**-59,03%**	**-25 000**	**21,19%**
Cizí zdroje	2 376 000	2 835 000	3 025 000	**459 000**	**19,32%**	**190 000**	**6,70%**
Reservy	0	0	0	**0**	**#DIV/0!**	**0**	**#DIV/0!**
Dlouhodobé závazky	0	0	0	**0**	**#DIV/0!**	**0**	**#DIV/0!**
Krátkodobé závazky	2 376 000	2 835 000	2 788 000	**459 000**	**19,32%**	**-47 000**	**-1,66%**
Bankovní úvěry a výpomoci	0	0	237 000	**0**	**#DIV/0!**	**237 000**	**#DIV/0!**
Ostatní pasiva	23 000	34 000	40 000	**11 000**	**47,83%**	**6 000**	**17,65%**

Zdroj: společnost „TELEMUZ s.r.o.“

Tabulka č.12: Analýzy vertikálních pasiv společnosti

Údaje jsou v Kč, respektivě v %	2006	2007	2008	2006	2007	2008
Pasiva celkem	2 031 000	2 369 000	2 412 000	**100,00%**	**100,00%**	**100,00%**
Vlastní kapitál	-368 000	-500 000	-653 000	**-18,12%**	**-21,11%**	**-27,07%**
Základní kapitál	100 000	100 000	100 000	4,92%	4,22%	4,15%
Kapitálové fondy	0	0	0	0,00%	0,00%	0,00%
Reservní fondy	10 000	10 000	10 000	-2,72%	-2,00%	-1,53%
Výsledky hospodaření minulých let	-190 000	-492 000	-620 000	-190,00%	-492,00%	-620,00%
Výsledek hosp. běž. účet. obd. po zdanění	-288 000	-118 000	-143 000	-14,18%	-4,98%	-5,93%
Cizí zdroje	2 376 000	2 835 000	3 025 000	**116,99%**	**119,67%**	**125,41%**
Reservy	0	0	0	0,00%	0,00%	0,00%
Dlouhodobé závazky	0	0	0	0,00%	0,00%	0,00%
Krátkodobé závazky	2 376 000	2 835 000	2 788 000	116,99%	119,67%	115,59%
Bankovní úvěry a výpomoci	0	0	237 000	0,00%	0,00%	9,83%
Ostatní pasiva	23 000	34 000	40 000	**1,13%**	**1,44%**	**1,66%**

Zdroj: společnost „TELEMUZ s.r.o.“

Z analýz tržeb vyplývá, že tržby meziročně stagnovaly, v roce 2007 dokonce poklesly. Tuto situaci lze přičíst všeobecné ekonomické situaci v oboru, který se potýká s poklesem zakázek. Nejvyšší podíl na celkových výnosech činí tržby z prodeje vlastních služeb. V roce 2006 byl jako doplňkový příjem i příjem z prodeje elektro materiálu a zboží.

Náklady meziročně klesají, což je působeno hlavně snížením počtu zaměstnanců a změnou DPH.

Je možné vysledovat růst nákladů na materiál a energie (výkonová spotřeba), ke kterému došlo pravděpodobně (chybí slovo) cen vstupu, ale může se jednat i o neefektivní využití zdrojů.

Vzhledem k tomu, že firma je malá CF nesleduje, a proto není možné sledovat čistý peněžní tok.

3.1.1 Analýza poměrových ukazatelů

Okamžitá likvidita

$$\text{Okamžitá likvidita (likvidita 1. stupně)} = \frac{\text{Finanční majetek}}{\text{Krátkodobé závazky}}$$

Tabulka č.13:Tabulka okamžité likvidity společnosti za roky 2006 - 2008

okamžitá likvidita	2006	2007	2008
finanční majetek	149 000	114 000	158 000
krátkodobé závazky	2 376 000	2 635 000	2 788 000
výsledek	**0,06271**	**0,04326**	**0,05667**

Zdroj: společnost „TELEMUZ s.r.o.“

Doporučené hodnoty okamžité likvidity jsou 0,2 až 0,6.

Dosažené výsledky ukazují na relativně dobré hospodaření s kapitálem.

Pohotová likvidita

$$\text{Pohotová likvidita (likvidita 2. stupně)} = \frac{\text{Oběžná aktiva - zásoby}}{\text{Krátkodobé závazky}}$$

Tabulka č.14: Tabulka pohotové likvidity společnosti za roky 2006 - 2008

pohotová likvidita	2006	2007	2008
oběžná aktiva	1 807 000	2 273 000	1 997 000
zásoby	408 000	432 000	538 000
krátkodobé závazky	2 376 000	2 635 000	2 788 000
výsledek	**0,58880**	**0,69867**	**0,52331**

Zdroj: společnost „TELEMUZ s.r.o.“

Doporučené hodnoty pohotové likvidity jsou od 1 až 1,5.

Vzhledem k tomu, že firma se pohybuje ve výsledcích pod 1, znamená to prvotní platební neschopnost. Příčinu vidíme v krátkodobých závazcích, kde podstatnou složkou jsou závazky ke společníkům.

Běžná likvidita

$$\text{Běžná likvidita (likvidita 3. stupně)} = \frac{\text{Oběžná aktiva}}{\text{Krátkodobé závazky}}$$

Tabulka č.15 běžné likvidity: Tabulka běžné likvidity společnosti za roky 2006 - 2008

běžná likvidita	2006	2007	2008
oběžná aktiva	1 807 000	2 273 000	1 997 000
krátkodobé závazky	2 376 000	2 635 000	2 788 000
výsledek	**0,76052**	**0,86262**	**0,71628**

Zdroj: společnost „TELEMUZ s.r.o.“

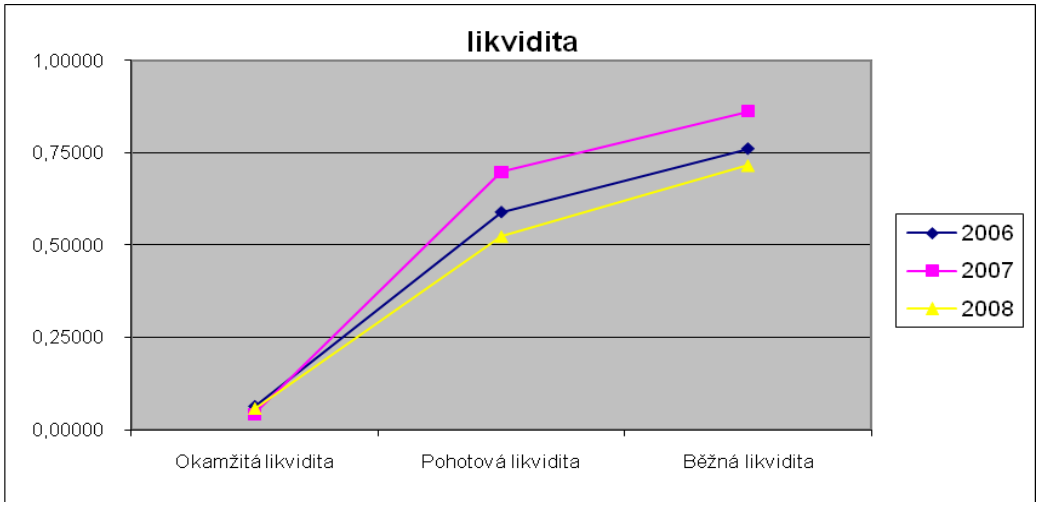
Doporučené hodnoty běžné likvidity jsou od 2 až 3, což je hodnota finančně zdravých firem. Pro zhodnocení můžeme použít odůvodnění, jako u pohotové likvidity.

Tabulka č.16: Celková likvidita společnosti za roky 2006 -2008

	2006	2007	2008
Okamžitá likvidita	*0,06271*	*0,04326*	*0,05667*
Pohotová likvidita	*0,58880*	*0,69867*	*0,52331*
Běžná likvidita	*0,76052*	*0,86262*	*0,71628*

Zdroj: společnost „TELEMUZ s.r.o.“

Graf č.2: Znázornění sumy likvidit společnosti za roky 2006 -2008:



Zdroj: společnost „TELEMUZ s.r.o.“

3.1.2 Analýza zadluženosti firmy

Celkové zadluženost

$$\text{Celková zadluženost} = \frac{\text{Cizí zdroje}}{\text{Aktiva celkem}}$$

Tabulka č.17: Tabulka celkové zadluženosti společnosti za roky 2006 -2008

celková zadluženost	2006	2007	2008
cizí zdroje	*2 376 000 Kč*	*2 835 000 Kč*	*3 025 000 Kč*
aktiva celkem	*2 031 000 Kč*	*2 369 000 Kč*	*2 412 000 Kč*
výsledek	***1,16987***	***1,19671***	***1,25415***

Zdroj: společnost „TELEMUZ s.r.o.“

Ukazatel se nazývá „Ukazatel věřitelského rizika“. V případě likvidace firmy roste riziko věřitelů poměrně růstu její zadluženosti. Vzhledem k tomu, že sledovaná firma má tento ukazatel od 116 do 125%, jedná se o firmu, která je pro věřitele značně nezajímavá.

3.1.3 Koeficient samofinancování

$$\text{Koeficient samofinancování} = \frac{\text{Vlastní kapitál}}{\text{Aktiva celkem}}$$

Tabulka č.18: Tabulka koeficientu samofinancování společnosti za roky 2006 -2008

koeficient samofinancování	2006	2007	2008
vlastní kapitál	*-368 000 Kč*	*-500 000 Kč*	*-653 000 Kč*
aktiva celkem	*2 031 000 Kč*	*2 369 000 Kč*	*2 412 000 Kč*
výsledek	***-0,18119***	***-0,21106***	***-0,27073***

Zdroj: společnost „TELEMUZ s.r.o.“

Aktiva u této firmy jsou financována vlastním kapitálem téměř v zanedbatelné míře.

3.1.4 Doba splácení dluhu

$$\text{Doba splatnosti dluhu} = \frac{\text{Cizí zdroje – finanční majetek}}{\text{Provozní Cash – Flow (potenciální diskont Cash – Flow)}}$$

Tabulka č.19: Tabulka doby splácení dluhu společnosti za roky 2006 -2008

doba splácení dluhu	2006	2007	2008
cizí zdroje	*2 376 000 Kč*	*2 835 000 Kč*	*3 025 000 Kč*
finanční majetek	*149 000 Kč*	*114 000 Kč*	*158 000 Kč*
provozní Cash-flow	*1 Kč*	*1 Kč*	*1 Kč*
výsledek	***2 375 999,00000***	***2 834 999,00000***	***3 024 999,00000***

Zdroj: společnost „TELEMUZ s.r.o.“

Dobu splácení dluhu nesledujeme u uvedené firmy, z důvodu nesledování Cash – Flow.

3.1.5 Úrokové krytí

$$\text{Úrokové krytí} = \frac{\text{EBIT}}{\text{Nákladové úroky}}$$

Tabulka č.20: Tabulka úrokového krytí společnosti za roky 2006 -2008

úrokové krytí	2006	2007	2008
EBIT	-288 000 Kč	-118 000 Kč	-132 000 Kč
nákladové úroky	0 Kč	0 Kč	3 000 Kč
výsledek	#DIV/0!	#DIV/0!	-44,00000

Zdroj: společnost „TELEMUZ s.r.o.“

Tento ukazatel nelze prozatím hodnotit vzhledem k tomu, že v roce 2006 a 2007 neměla firma žádný úvěr ani výpomoc až v roce 2008 byl úvěr poskytnut.

3.1.6 Analýza řízení aktiv

Obrat celkových aktiv

$$\text{Obrat celkových aktiv} = \frac{\text{Tržby}}{\text{Aktiva celkem}}$$

Tabulka č.21: Tabulka obratu celkových aktivit společnosti za roky 2006 -2008

obrat celkových aktiv	2006	2007	2008
tržby	5 007 000	4 853 000	5 165 000
aktiva celkem	2 031 000	2 369 000	2 412 000
výsledek	2,4652880355	2,0485436893	2,1413764511

Zdroj: společnost „TELEMUZ s.r.o.“

Doporučená hodnota je 1,6 až 3. Vzhledem k dosaženým hodnotám je sledovaná firma v tomto ukazateli v pořádku.

Obrat stálých aktiv

$$\text{Obrat stálých aktiv} = \frac{\text{Tržby}}{\text{Stálá celkem}}$$

Tabulka č.22: Tabulka obratu stálých aktiv společnosti za roky 2006 -2008

obrat stálých aktiv	2006	2007	2008
tržby	5 007 000	4 853 000	5 165 000
stálá aktiva			
výsledek	#DIV/0!	#DIV/0!	#DIV/0!

Zdroj: společnost „TELEMUZ s.r.o.“

Obrat zásob

$$\text{Obrat zásob} = \frac{\text{Tržby}}{\text{Zásoby}}$$

Tabulka č.23: Tabulka obratu zásob společnosti za roky 2006 -2008

obrat zásob	2006	2007	2008
tržby	5007000	4853000	5165000
zásoby	408 000	432 000	538 000
výsledek	**12,2720588235**	**11,2337962963**	**9,6003717472**

Zdroj: společnost „TELEMUZ s.r.o.“

Obrat pohledávek

$$\text{Obrat pohledávek} = \frac{\text{Tržby}}{\text{Obchodní pohledávky}}$$

Tabulka č.24: Tabulka obratu pohledávek společnosti za roky 2006 -2008

obrat pohledávek	2006	2007	2008
tržby	5 007 000	4 853 000	5 165 000
obchodní pohledávky	1 240 000	1 716 000	1 290 000
výsledek	**4,0379032258**	**2,8280885781**	**4,0038759690**

Zdroj: společnost „TELEMUZ s.r.o.“

1.1. ***Analýza rentability***

ROI = hospodářský výsledek před zdaněním

$$\text{ROI} = \frac{\text{hospodářský výsledek před zdaněním + nákladové úroky}}{}$$

$$\text{ROI} = \frac{\text{Hospodářský výsledek před zdaněním + nákladové úroky}}{\text{Celkový kapitál}}$$

Tabulka č.25: Tabulka ROI společnosti za roky 2006 -2008

ROI	2006	2007	2008
hospodářský výsledek před zdaněním + nákladové úroky	*- 288 000,00 Kč* *- Kč*	*- 118 000,00 Kč* *- Kč*	*- 135 000,00 Kč* *3 000,00 Kč*
celkový kapitál	*- 368 000,00 Kč*	*- 500 000,00 Kč*	*- 653 000,00 Kč*
výsledek	**0,78261**	**0,23600**	**0,20674**

Zdroj: společnost „TELEMUZ s.r.o.“

Doporučené hodnoty ROI > 0,15 ukazuje na velmi dobré výsledky.

ROI je vhodné k porovnání různě zdaněných a zadlužených podniků, protože nebere v úvahu ani úroky ani daně. ROI je v celém sledovaném období větší než doporučená hodnota 0,15, což znamená, pozitivní vývoj firmy. Obecně platí, že čím vyšší ROI tím lepší.

ROA = ukazatel rentability celkových aktiv

$$ROA = \frac{\text{Hospodářský výsledek po zdaněním}}{\text{Celkový aktiva}}$$

Tabulka č.26: Tabulka ROA společnosti za roky 2006 -2008

ROA	2006	2007	2008
hospodářský výsledek po zdanění	- 288 000,00 Kč	- 118 000,00 Kč	- 143 000,00 Kč
celková aktiva	2 031 000,00 Kč	2 369 000,00 Kč	2 412 000,00 Kč
výsledek	**-0,14180**	**-0,04981**	**-0,05929**

Zdroj: společnost „TELEMUZ s.r.o.“

ROE = ukazatel rentability vlastního kapitálu

$$ROE = \frac{\text{Hospodářský výsledek po zdaněním}}{\text{Vlastní kapitál}}$$

Tabulka č.27: Tabulka ROE společnosti za roky 2006 -2008

ROE	2006	2007	2008
hospodářský výsledek po zdanění	- 288 000,00 Kč	- 118 000,00 Kč	- 143 000,00 Kč
vlastní kapitál	- 368 000,00 Kč	- 500 000,00 Kč	- 653 000,00 Kč
výsledek	**0,78261**	**0,23600**	**0,21899**

Zdroj: společnost „TELEMUZ s.r.o.“

ROE hodnotí přínos pro vlastníky. Vzhledem k tomu, že hodnoty ROE jsou téměř shodné s hodnotami ROI, firma netvoří příliš velkou hodnotu pro vlastníky.

Finanční páka = ROE > ROA

$$\text{Finanční páka} = \frac{\text{Celková aktiva}}{\text{Vlastní kapitál}}$$

Tabulka č.28: Tabulka finanční páky společnosti za roky 2006 -2008

finanční páka	2006	2007	2008
celková aktiva	2 031 000,00 Kč	2 369 000,00 Kč	2 412 000,00 Kč
vlastní kapitál	- 368 000,00 Kč	- 500 000,00 Kč	- 653 000,00 Kč
výsledek	**-5,51902**	**-4,73800**	**-3,69372**

Zdroj: společnost „TELEMUZ s.r.o.“

3.2 Řešení nového komunikačního a informačního systému

V předcházejících kapitolách byl nový komunikační a informační systém [14] dostatečně teoreticky popsán se všemi riziky, které působí z vnějšího i vnitřního prostředí.

V této kapitole bych chtěl provést finanční analýzu podnikatelského záměru, i když navrhovaný systém nepřichází pro státní správu v úvahu. Rozpočet jako základní dokument pro investiční záměr musí být vytvořen. Tato ucelená finanční dokumentace bude sloužit k závěrečnému rozhodnutí zda, podnikatelský záměr realizovat či zamítnout.

3.3 Metriky pro informační systém

3.3.1 Výpočet hodnoty informace podle Shannona

Podle Shannona[15], [16], [24] je hodnota informace založena na pravděpodobnosti výskytu symbolu ve zprávě, pokud všechny zprávy mají stejnou pravděpodobnost podle vzorce:

$$I = \log_2 N \text{ bit}$$

ale pokud všechny zprávy nemají stejnou pravděpodobnost[24] vychází ze vzorce:

$$I = -n * \sum_{i=1}^{s} p_i \log_2 p_i \text{ bit}$$

Měřitelnost informace je založena na růstu a klesání entropie, která vyjadřuje míru nejistoty. Klesá-li entropie, roste hodnoty informace a naopak. Entropie znamená míru rozmanitosti systému, kterým informace prochází. Jestliže v systému existuje zákonitost, bezpečnost a řád, klesá rozmanitost možností, a tudíž lze konstatovat, že informace je kvantitativní mírou vnitřních zákonitostí a následně s poklesem rozmanitosti klesá množství informace v systému. Informace je imaginární veličinou, neměřitelnou, přesně nedefinovatelnou, kterou lze ale získat materiální kvalitu vůči konkurenci. Informace je odvislá od mnoha parametrů:

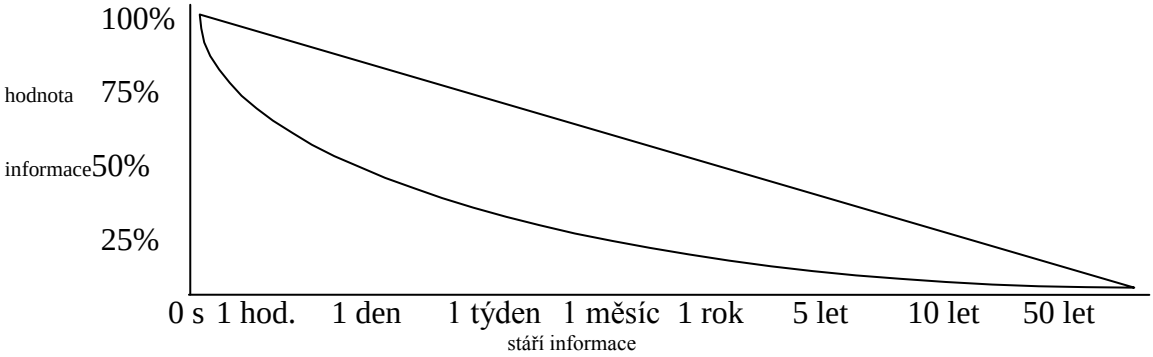
- Hodnota, která je závislá na mnoha vztazích, jednotka informace je nejistá, neobecná,

- Lze stanovit jednotku jen k určitému měření,
- Informace je to, co přijímáme srozumitelnou formou pro lidské zdroje a mající hodnotu:
    - Informační – kvantitativní, informace je jedna zpráva (údaj)
    - Kybernetický – teoretický, matematická teorie komunikace (kolik informace obsahuje tato část dat)

Informace ve zprávě je definována jako záporný dvojkový logaritmus její pravděpodobnosti.

Finanční hodnota takto ztracených dat ve většině případů daleko přesahuje hodnotu hardwaru i softwaru, na kterém jsou uložena a zpracovávána. A to i v případě, že je máme zálohovány, a jsme schopni je obnovit a používat je dále.

Graf č.3: Hodnota informace vzhledem k jejímu stáří



Zdroj: www:MVCR.cz

Analýza hodnoty informace [25] tvoří očekávaný užitek informace (EU – Expected Utility). Očekávaný užitek nemůžeme chápat normativně, ale v souvislostech zohledňující individuální přístup jednotlivých osob k informaci jako celku.

Hodnotu informace[9] lze vyjádřit ex-ante jako náklad C_o na informaci, při její důležitosti, která vychází z očekávaného zisku. Podobně lze hodnotu informace lze vyjádřit ex-post jako náklad C_o srovnatelný s ekvivalentem jistotou informace, při rozhodování bez informací.

3.3.2 Výpočet hodnoty lidského kapitálu - HDI

Index lidského kapitálu[26] (Human development index) je pokus o vyjádření kvality lidského života za pomocí základní porovnatelných faktorů (střední délka života, gramotnost, HDP na jednoho obyvatele v paritě kupní síly). Metoda pro výpočet HDI

obecně proměňuje surovou proměnnou „x“ do jednotky-volný index , které je v intervali <0;1>, pro uvedenou definici existuje následující vzorec:

3.3.2.1 Index očekávané délky života (Life Expectancy Index)

$$x - index = \frac{x - \min(x)}{\max(x) - \min(x)}$$

Hodnotu lidského kapitálu lze vypočítat[14] z následujících vztahů:

3.3.2.2 Index očekávané délky života (Life Expectancy Index)

$$LEI = \frac{LE - 25}{85 - 25}$$

3.3.2.3 Index vzdělání (Education Index)

$$EI = \frac{2}{3} * ALI + \frac{1}{3} * GEI$$

3.3.2.4 Index gramotnosti populace (Adult Literacy Index)

$$ALI = \frac{ALR - 0}{100 - 0}$$

3.3.2.5 Index zápisu do školy (Gross Enrollment Index)

$$GEI = \frac{CGER - 0}{100 - 0}$$

3.3.2.6 Index HDP (GDP Index)

$$GDP = \frac{\log(GDPpc) - \log(100)}{\log(40000) - \log(100)}$$

3.3.2.7 Výpočet hodnoty vzdělání a její návratnost

Ve své podnikatelském záměru se budu zabývat i výpočtem hodnoty vzdělání a její návratnosti[26] v čase a využití intelektuálu vůči zaměstnavateli, který hodnotu vzdělání ohodnocuje vyšším postavením a funkcí, s následnou vyšší finanční hodnotou. Pro vzdělání je nutné započítat náklady na vzdělání a výnosy, které z tohoto plynou, viz rovnice[15]:

$$\sum_{t=G-E}^{R-E} (E_1 - E_0) * (1 + r^*) - \sum_{t=G-E}^{R-E} (E_0 + C) * (1 + r^*) = 0$$

[14] LE- střední délka života (Life Expectancy); ALR-gramotnost (Adult Literacy Rate); CGER-kombinovaný poměr do škol (Combined Gross Enrolment Ratio); GDPpc HDP na 1 obyvatele (GDP per capita at PPP in USD)

[15] Uvedená rovnice představuje výpočet míry návratnosti investice do vzdělání (vnitřní výnosová procenta) jedná se **plnou metodu**

kde:

$E_0(t)$ = výdělková funkce pro předterciální vzdělání,

$E_1(t)$ = výdělková funkce pro terciální vzdělání[16],

C(t) = funkce přímých nákladů,

E = věk začátku terciálního vzdělávání,

G = věk při ukončení terciálního vzdělávání,

R = věk při odchodu do důchodu,

r^* = míra návratnosti investice do vzdělávání,

S_h = délka terciálního vzdělávání, S_h = G-E,

N = roky pracovního života zaměstnance, N = R-G

3.3.3 Výpočet hodnoty lidského kapitálu v České republice

Tabulka č.29: HDI v roce 2007

Pořadí zemí v HDI v roce 2007		Průměrná délka života	Kombinovaná primární a sekundární pravidlo	GDP na hlavu	Index průměrní délky života	Vzdělávací index	GDP index	Lidský vývojový index HDI
1.	Norsko	78,4	97	28,433	0,89	0,98	0,94	0,939
2.	Austrálie	78,8	116	24,574	0,99	0,99	0,92	0,936
3.	Kanada	78,7	97	26,251	0,98	0,98	0,93	0,936
4.	Švédsko	79,6	101	22,636	0,99	0,99	0,90	0,936
5.	Belgie	78,2	109	25,443	0,99	0,99	0,92	0,936
6.	USA	76,2	95	31,872	0,98	0,98	0,96	0,934
7.	Holandsko	76/8	89	27,835	0,96	0,96	0,94	0,932
8.	Dánsko	79,1	102	24,215	0,99	0,99	0,92	0,931
9.	Japonsko	80,8	82	24,895	0,93	0,96	0,92	0,928
10.	Finsko	77,4	103	23,096	0,99	0,99	0,91	0,925
32.	**ČR**	**74,7**	**70**	**13,018**	**0,83**	**0,89**	**0,89**	**0,844**

Zdroj: www.czp.cuni.cz

[16] Vzdělanost společnosti

3.3.4 Stanovení hodnoty a návrh hardware

Investice společnosti do pořízení hardwaru, je velmi složitým, ekonomickým a manažerským rozhodnutím, které je nutno učinit v daný okamžik situaci, čase, neovlivnitelným vnějším a vnitřním vlivům.

Hardwarové složení komunikačního a informačního systému je nutno technicky a programově rozhodnout, jelikož každé rozhodnutí je ovlivněnou zdrojem financování systému. Při rozhodování je nutné a nezbytné stanovit prioritu používání a využivatelnosti počítačové sestavy. Jaké informace a data budou zpracovávány, v jakém časovém horizontu a s jakou frekvencí. Nejdůležitější a zásadní je, v jakém utajeném režimu budou pracovat sestavy.

3.3.5 Technické parametry - hardware

- Server: – Intel Xeon, 3 GHz, 4 GB RAM, HDD 5x 142GB SCSI Ultra Hot Plug, zapojených v RAID 5, SCSI zálohovací pásková mechanika – 400GB,
- Pracovní stanice: – Intel – Pentium Core 2 – Duo, 3 GHz, 2 GB RAM, HDD 250GB,
- Síťová multifunkční laserová barevná tiskárna,
- Napěťové zálohovací zdroje UPS 2500 kW

Tabulka č.30: Návrh finančního zajištění pracoviště komunikačního a informačního systému od společnosti „TELEMUZ s.r.o.“

Název produktu	100 Mega	Czech Computer	AutoCont	Auroton	Secunet	SINA
Server Intel Xeon	140 000,-Kč	142 500,-Kč	138 000,-Kč	141 000,-Kč	0,-Kč	0,-Kč
Pracovní stanice uživatele	35 000,-Kč	37 000,-Kč	40 000,-Kč	38 000,-Kč	0,-Kč	0,-Kč
Multifunkční zařízení	40 000,-Kč	38 000,-Kč	35 000,-Kč	45 000,-Kč	0,-Kč	0,-Kč
Kryptografický prostředek	0,-Kč	0,-Kč	0,-Kč	0,-Kč	225 000,-Kč	180 000,-Kč
IP telefon	14 000,-Kč	15 000,-Kč	15 500,-Kč	15 000,-Kč	0,-Kč	0,-Kč
Čtečka ID karet	1 500,-Kč	1 200,-Kč	1 200,-Kč	1 300,-Kč	0,-Kč	0,-Kč
Zálohovací zdroje UPS	30 000,-Kč	35 000,-Kč	0,-Kč	32 000,-Kč	0,-Kč	0,-Kč
Zálohovací hardware	60 000,-Kč	65 000,-Kč	59 000,-Kč	58 000,-Kč	0,-Kč	0,-Kč
Rack 19“ - 42 U	80 000,-Kč	85 000,-Kč	115 000,-Kč	80 000,-Kč	0,-Kč	0,-Kč
Celkem návrh:	**405 000,-Kč**	**418 700,-Kč**	**403 700,-Kč**	**390 300,-Kč**	**225 000,-Kč**	**180 000,-Kč**

Zdroj: společnost „TELEMUZ s.r.o.“

Obrázek č.4: Návrh pracoviště komunikačního a informačního systému od společnosti „TELEMUZ s.r.o.“

Zdroj: společnost „TELEMUZ s.r.o.“

Situace v oblasti tzv. „železa“ neboli technického vybavení hardwaru je v současné době chráněna jako věc movitá podle zákona č. 40/1964 Občanského zákona §118, odst.1, a §119[33]. Je tedy snadněji uchopitelnou nežli v případě nehmotného produktu softwaru. Takto definovaný majetek lze finančně a ekonomicky ohodnotit, s následným účetním a daňovým odpisováním podle druhu a typu společnosti a jejich podnikatelských aktivit. U státní správy je tento problém neřešitelný, jelikož hardware musí pracovat až za hranice svých možností a pak je nahrazen novým výkonnějším, efektivnějším a ekonomicky přijatelným hardwarem.

3.3.6 Software

Investice společnosti do pořízení softwaru[17], umožní společnosti, pracovním týmům i uživatelům zvyšovat produktivitu, bezpečnost a identitu. Za pomocí licencovaného (viz příloha č.2) software, v kontextu s bezpečnostní politikou, lze dosáhnout nevyčíslitelných hodnot, které jsou zužitkovány až v případě bezpečnostního ohrožení chráněného zájmu.

Prostou analýzou rizik, s přihlédnutím na ekonomické, finanční a bezpečnostní aktivity[13], je z hlediska bezpečnosti nejdůležitější zajistit správný a licencovaný software.

Pokud společnost neinvestuje do legálního softwaru, hrozí ztráta dat, porucha hardwarového vybavení nebo uživatelské poškození dat z důvodu neprovádění zálohování dat. Dále může docházet i k narušení integrity dat a zneužití informací, jak ze strany zaměstnanců firmy, tak i cestou nezabezpečeného internetového připojení od konkurenčních firem nebo zaplaceným hackerem. Může docházet k nekontrolovanému úniku dat pomocí interních mechanik nebo odesláním pomocí Internetu. Pracovní stanice společnosti jsou vystaveny „rádoby odborníkům" a uživatelům komunikačního a informačního systému, kteří mohou instalovat podbízené programy z odborné literatury nebo nelegálně získané z Internetu či jiných zdrojů, a tím způsobit havárii a kompromitaci dat a informací v informačním systému.

Tyto nedostatky v zabezpečení informačního systému mohou zapříčinit nenahraditelné ztráty z důvodu nedostupnosti, změny integrity a zneužití informací uložených na lokálních discích pracovních stanic.

Při používání těchto kombinací software se společnost, aniž by přesně monitorovala, co je nainstalováno na pracovních stanicích, vystavuje nebezpečí kolize s autorským zákonem a „pirácky" nainstalovaný softwarem může způsobit víc škod než užitku. Zjednodušeně řečeno: „*Softwaru, který si člověk legálně nekoupí nic neužije, pokud si ho nekoupí"*[17] a nebo *„pokud jej chceme, používat v práci, musíme za něj zaplatit"*. Zároveň není stanovena zodpovědnost konkrétních osob za legálnost instalovaných aplikací.

3.3.7 Technické parametry - software

- Server MS Small Business Server 2003 Premium Edition[12], [19], [28],
- MS Windows XP Professional na pracovních stanicích[19],
- MS Windows XP VISTA na pracovních stanicích
- MS Office 2007 Professional,
- Eset Smart Secure – antivirová ochrana na pracovních stanicích,

[17] zdroj: časopis COMPUTER 6/07, vydává Moraviapress, a.s., str. 16, registrace ISSN 1210-8790, MK ČR E 6901

Tabulka č.31: Porovnání finančních nákladů na software na 1 PC

Název produktu	100 Mega	Czech Computer	AutoCont	ComSoft	Auroton
Server MS Small Business Server 2003 Premium Edition – licencí pro 5 klientů	25 000,-Kč	25 500,-Kč	24 000,-Kč	25 000,-Kč	24 500,-Kč
Client Access licence (CAL)	15 000,-Kč	14 900,-Kč	14 500,-Kč	15 000,-Kč	15 500,-Kč
MS WIN VISTA Business	4 300,-Kč	4 000,-Kč	4 100,-Kč	4 300,-Kč	4 000,-Kč
MS OFICCE 2007 Pro Small Business	14 000,-Kč	14 000,-Kč	14 500,-Kč	14 300,-Kč	14 000,-Kč
Antivirový program 1 licence	1 400,-Kč	1 200,-Kč	1 500,-Kč	1 200,-Kč	1 500,-Kč
Program na bezpečné mazání	1 000,-Kč	900,-Kč	1 000,-Kč	1 100,-Kč	1 000,-Kč
Crypto + ProID pro 1. stanici	1 200,-Kč	1 100,-Kč	1 200,-Kč	1 000,-Kč	1 000,-Kč
Celkem návrh:	**61 900,-Kč**	**61 100,-Kč**	**60 800,-Kč**	**61 900,-Kč**	**61 500,-Kč**

Zdroj: společnost „TELEMUZ s.r.o.“

Tabulka č.32: Porovnání finančních nákladů na software na 5 PC

Název produktu	100 Mega	Czech Computer	AutoCont	ComSoft	Auroton
Server MS Small Business Server 2003 Premium Edition – licencí pro 5 klientů	25 000,-Kč	25 500,-Kč	24 000,-Kč	25 000,-Kč	24 500,-Kč
Client Access licence (CAL)	15 000,-Kč	14 900,-Kč	14 500,-Kč	15 000,-Kč	15 500,-Kč
MS WIN VISTA Business	21 500,-Kč	20 000,-Kč	20 500,-Kč	21 500,-Kč	20 000,-Kč
MS OFICCE 2007 Pro Small Business	70 000,-Kč	70 000,-Kč	72 500,-Kč	71 500,-Kč	70 000,-Kč
Antivirový program 1 licence	7 000,-Kč	6 000,-Kč	7 500,-Kč	6 000,-Kč	7 500,-Kč
Program na bezpečné mazání	5 000,-Kč	4.500,-Kč	5 000,-Kč	5 500,-Kč	5 000,-Kč
Crypto + ProID pro 1. stanici	6 000,-Kč	5 500,-Kč	6 000,-Kč	5 000,-Kč	5 000,-Kč
Celkem návrh:	**149 500,-Kč**	**146 400,-Kč**	**150 000,-Kč**	**149 500,-Kč**	**147 500,-Kč**

Zdroj: společnost „TELEMUZ s.r.o.“

Situace v oblast tzv. „myšlenky“ neboli programového vybavení softwaru v současné době je chráněna[17] jako věc nemovitá[32] podle zákona č. 121/2000Sb., autorský zákon podle § 22, odst. 1, písm. g), zákona č. 586/1992 Sb., o daních z příjmů, zákon č. 207/2000 Sb., o ochraně průmyslových vzorů, zákon č. 527/1990 Sb., o vynálezech, průmyslových vzorech a zlepšovacích návrzích[31], zákon č. 478/1992 Sb., o užitných vzorech. U softwaru rozlišujeme dvě podoby:

- Zdrojový program – program, jak jej napsal programátor
- Strojový kód- spustitelná program, založený na zdrojovém programu

Platí, že zdrojový program je primární, hlavní a určující cenu, životnost, efektivnost, bezpečnostní standardy a rizika napadení. Program je posloupnost nul a jedniček (bitů).

Od jednoduchého zdrojového programu a jednoduché posloupnosti se kombinací můžeme dostat k dokonalejším produktům tzv. programovým produktům, vybavením, systémům a prostředkům. Tento výrobek musíme v souvislostech informační bezpečnosti chápat jako komplexnější a složitější než je samostatný program. A zde v 95% dochází k jeho ohrožení, zneužití, poškození nebo zničení konkurencí, neloajálním subjektem.

3.3.8 Kryptografické prostředky

Kryptografické mechanizmy[5] jsou využívány v nejrůznějších počítačových a komunikačních systémech v kombinaci s prostředím. Investice a úroveň musí být zvolena tak, aby byla zajištěna dostatečná ochrana dat a informací v souvislosti s požadavky, prostředím a poskytování služeb. Neúměrnost investicí společnosti do pořízení kryptografických modulů vyvolá řetězovou reakci a odezvu o plýtvání s finančními prostředky jen do doby, kdy tyto kryptografické moduly v souběhu s dalšími opatřeními zabrání, ochrání a podají managementu data a informace v časové výhodnosti a získají podnikatelskou výhodnost před konkurencí.

Implementace kryptografických modulů ve formě hardwarových, softwarových a firmwarových modulů jsou ve standardu (FIPS140) definovány jako čtyři kvalitativní kategorie kryptografických modulů. Kombinace těchto modulů pokrývá celé spektrum bezpečnosti.

V současné době je výpočet hodnoty kryptografických mechanizmů založen na teoretickém ohrožení, které je ohodnoceno v zákoně č. 412/2005 Sb., část druhá, hlava I. § 1; 2. Investice musí být tudíž přiměřená a kontinuální vyvolaná nebezpečím. Kryptografické moduly a prostředky jsou finančně a morálně náročné, podléhají nejvyššímu stupni ochrany, a tudíž je velice těžké jejich vyčíslení.

Hodnota kryptografické ochrany informací a dat je vysoce specifickou záležitostí, kde je nutné vidět dlouholetou, intenzivní, odbornou a technickou vyspělost společnosti a pracovníků, kteří toto realizují. Hodnota těchto mechanizmů odráží vývoj,

testování, upgrady daleko před vlastním použitím a jen několik certifikovaných a specializovaných společností, kteří svou podnikatelskou živnost spojili s touto oblastí.

Lze konstatovat, že hodnota ochrany je vysoká v době, kdy probíhá standardní komunikace, ale okamžitě při výskytu incidentu, kompromitace, úniku informací a dat není cena tohoto produktu sledována. Důležité je jak kvalitně a rychle dokáže ochránit chráněná aktiva před konkurencí či terorismem.

Každá organizace je povinna svá citlivá data a informace chránit, zálohovat a veřejně je neposkytovat třetí osobě za účelem získání konkurenční výhody či dokonce zničení dalšího subjektu.

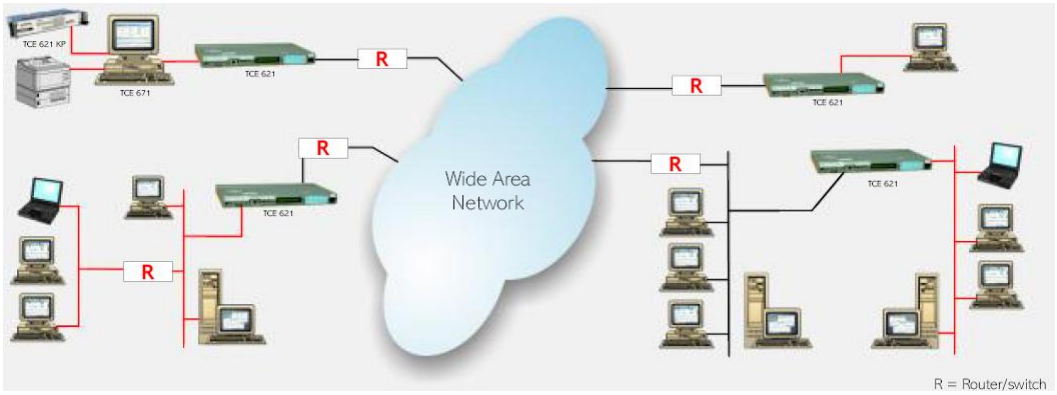
3.3.9 Technické parametry – kryptografické prostředky

- IP šifrátor TCE 621/C, následujícími parametry
  - Plně schopný spolupracovat s TCE 621, schváleno pro všechny stupně NATO a pro Norsko
  - Podpora dvou protokolů IPv4 a IPv6
  - Centralizovaný šifrátor spolupracující s TCE 671
  - Elektronická a ruční klíčová distribuce je dostupná
  - Transparentní síťová služba
  - Gigabitový výkon
  - Utajovaný protokol IETF AFC 2406-ESP
  - Plný duální provoz 600Mbit/s
  - Přenos 200 000 paketů za sekundu
  - Enviromentální parametry podle IEC 68-2, DEF-SWAN 07-55
  - Software lze zavést i po síti

Obrázek č.5: Šifrátor TCE 621

Zdroj: společnost „Thales Norway AS“; www.thalesgroup.com

Obrázek č.6: Návrh systémového propojení komunikačního a informačního systému ve státní správě



Zdroj: společnost „Thales Norway AS“; www.thalesgroup.com

- IP šifrátor SINA BOX s následujícími parametry:

Tabulka č.33: Porovnání šifrátoru SINA BOX podle stupně utajení

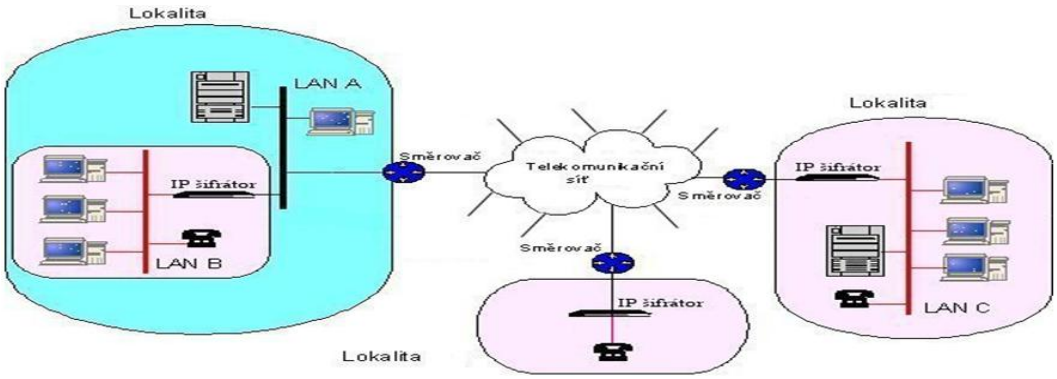
SINA		Pro klasifikovaná data ČR			Pro klasifikovaná data EU		
		VYHRAZENÉ	DŮVĚRNÉ	TAJNÉ	VYHRAZENÉ	DŮVĚRNÉ	TAJNÉ
SINA	BOX M	**ANO**	**ANO**	**ANO**	**NE**	**NE**	**NE**
SINA	BOX P	**ANO**	**ANO**	**ANO**	**ANO**	**ANO**	**ANO**
SINA	BOX S	**ANO**	**ANO**	**NE**	**ANO**	**ANO**	**NE**
SINA	BOX S BUSINESS	**ANO**	**NE**	**NE**	**ANO**	**NE**	**NE**

Zdroj: společnost „secunet s.r.o.“; www.secunet.com

Obrázek č.7: Šifrátor SINA BOX

Zdroj: společnost „secunet s.r.o.“; www.secunet.com

Obrázek č.8: Blokové schéma navrhovaného stavu komunikačního a informačního systému



Zdroj: společnost „TELEMUZ s.r.o.“

3.4 Bezpečnostní a provozní funkce nového komunikačního a informačního systému

V informačním systému společnosti jsou použity všechny zásady, minimální požadavky bezpečnosti informačního systému[11], [12], popsané v teoretické části diplomové práce.

Volitelné řízení přístupu uživatelů a skupin ke sdíleným prostředkům systému – jednoznačná identifikace uživatele předchází všem aktivitám uživatele. Uživatel se přihlásí pomocí uživatelského jména a hesla k doménovému řadiči, který k ověření a nastavení privilegií a zásad skupin používá jednotnou distribuovanou databázi Active Directory.

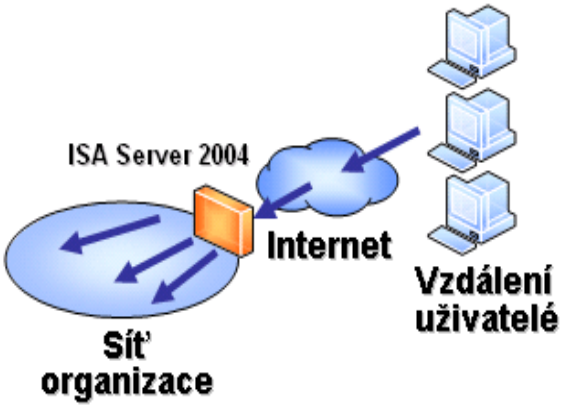
Bezpečnostní opatření systému zajistí, že jsou nepřetržitě zaznamenávány důležité informace o akcích prováděných uživateli a procesech běžících pod jejich účty. Toto bude zajištěno prostředky operačních systémů Microsoft Windows 2003 a Microsoft WIN XP a v některých případech rovněž na aplikační úrovni (například antivirová ochrana).

Systém technických a organizačních opatření zajišťuje, aby byly ošetřeny paměťové objekty před jejich dalším použitím, zejména před přidělením jinému subjektu, které znemožní zjistit jejich předchozí obsah. Opakované použití objektů bude řešeno použitým operačním systémem. U vyjímatelných médií budou stanovena přísná pravidla pro používání, předávání a ničení.

Bezpečnostní systém zajišťuje volitelné řízení přístupu k objektům na základě rozlišování a správy přístupových práv uživatele a identity uživatele nebo jeho členství ke skupině. Toto bude zajištěno prostředky OS nastavením bezpečnostních parametrů.

ISA Server[27], který je součástí Small Businnes Serveru Premium Edition, obsahuje komplexní bránu firewallu na aplikační vrstvě, která umožňuje bránit informační systém firmy před externími i interními útoky a hrozbami. Brána firewallu také poskytuje kontrolu klientů VPN (virtuální privátní sítě) a umožňuje tak chránit sítě před útoky přicházejícími přes připojení VPN.

Obrázek č.9: Schéma připojení informačního systému přes ISA Server 2004 s vnějším komunikačním prostředím



Zdroj: vlastní

Server bude vybaven zálohovací páskovou magnetickou mechanikou, která spolu se zálohovacím SW zajistí zálohování systémových a uživatelských dat. Vzhledem k použité zálohovací mechanice budou zálohovací úlohy prováděny v poloautomatickém režimu, kdy zodpovědná osoba bude vyměňovat magnetické pásky datových skladů. Bude vypracován zálohovací plán. Rovněž bude pravidelně testována funkčnost zálohování, prováděním zkušebních obnovovacích procesů. Zároveň bude vytvořena politika ukládání zálohovacích páskových médií na bezpečném místě mimo prostory firmy (bezpečnostní schránka banky).

Dostupnost dat k určitému dni je 14 dnů, plné zálohy jsou dostupné 28 dnů a zálohy prováděné podle předchozího odstavce jsou dostupné 52 týdnů.

Dále se provádí manuální zálohování auditních záznamů pracovních stanic a serveru minimálně 1x měsíčně.

Páska 11 se nevrací do čtyřtýdenního cyklu, ale označuje se pořadovým číslem (1-12), ukládá se na dobu 12 měsíců a uplynutí této doby se znovu použije.

Harmonogram zálohování uživatelských, systémových dat a databází probíhá podle tabulky, přičemž červeně jsou označeny plné zálohy a žlutě zálohy přírůstkové:

Tabulka č.34: Zálohování uživatelských, systémových dat a databází

Zálohovací plán	1. týden	2. týden	3. týden	4. týden
Pondělí	 Páska 1	 Páska 6	 Páska 1	 Páska 6
Úterý	 Páska 2	 Páska 7	 Páska 2	 Páska 7
Středa	 Páska 3	 Páska 8	 Páska 3	 Páska 8
Čtvrtek	 Páska 4	 Páska 9	 Páska 4	 Páska 9
Pátek	 Páska 5	 Páska 10	 Páska 5	 **Páska 11**

Zdroj: vlastní

Dále se provádí manuální zálohování auditních záznamů pracovních stanic a serveru minimálně 1x měsíčně.

Antivirový program je navržen tak, aby spolehlivě ochránil systém. Dokáže minimalizovat rizika napadení informačního systému před počítačovým virem, kontroluje příchozí i odchozí elektronickou poštu a zamezí šíření škodlivého software (spyware). Server antivirové ochrany bude aktualizován automaticky přes Internet od výrobce SW. Antivirová ochrana pracovních stanic bude instalovaná jako „spravovaná“, tedy veškeré bezpečnostní nastavení funkcí a aktualizace přebírá ze serveru antivirové ochrany. Vypnutí rezidentní ochrany a odinstalování antivirového SW je možné pouze na základě znalosti hesla k těmto úkonům.

Profily uživatelů jsou konfigurovány jako cestovní, což umožní uživatelům se přihlásit z libovolné pracovní stanice, bez omezení bezpečnosti a funkčnosti systému. Rovněž systém poskytuje zabezpečeným protokolem pružný vzdálený přístup vybraných zaměstnanců, při současném zajištění ochrany firemní sítě před nebezpečnými daty přenášenými přes síť.

Prostřednictvím aplikace MS SharePoint Service, která je součástí Small Businnes Server Premium Edition, se vytvoří interní firemní web (intranet) pro sdílení dokumentů a informací mezi uživateli firmy.

Informační systém zajišťuje robustní e-mailové řešení využívající Exchange Server 2003 a MS Outlook 2003. Pomocí jediného průvodce lze navíc snadno nakonfigurovat nastavení sítě, brány firewallu, zabezpečeného webu a e-mailu tak, aby bylo možné počítač s operačním prostředím Windows Small Business Server správně připojit k Internetu. To umožňuje správně nastavit připojení a zabezpečení již od samého začátku.

Tiskový server umožní sdílet síťový tisk všem uživatelů, odesílání faxových zpráv z počítačů přes multifunkční tiskové zařízení a příjem faxových zpráv pomocí e-mailu či na multifunkční tiskárnu. Všechny tyto aktivity jsou auditovány, zálohovány a vyhodnocovány kontrolními mechanizmy společnosti.

Komunikační a informační[13] systém společnosti je nastaven a provozován podle standardů NBÚ a standardů NATO je implementován na podmínky standardní ochrany informací pro využití a spolupráci České republiky se státy EU.

V následující tabulce jsem se snažil finančně zhodnotit náklady na jednotlivé pracovní činnosti, které jsou nezbytně nutné pro provozování systému. Určitě není 100% zachycena veškerá činnost při realizaci podnikatelského záměru a finanční ocenění vychází z nabídkového řízení a podkladů firem, které se touto problematikou dlouhodobě zabývají. Cenová nabídka odpovídá možnostem prodejnosti a realizovatelnosti systému pro státní správu.

Tabulka č.35: Náklady vynaloženy na zprovoznění systému

Název činnosti	Náklady na činnost	Poznámka
Zpracování bezpečnostní dokumente a projektu	1 000 000,-Kč	
Zavedení a dodržování bezpečnostní politiky na centru 600*1200	720 000,-Kč	
Zavedení a zkontrolování bezpečnostní politiky na 5 ks PC	10 000,-Kč	
Náklady na školení správců a bezpečnostních pracovníků systému	500 000,-Kč	
Náklady na objektovou bezpečnost na 5 ks PC	12 500,-Kč	
Náklady na síťové prostředí systému na 100m	50 000,-Kč	
Náklady na administrativní bezpečnost	5 000,-Kč	
Náklady mzdové pracoviště dohledu (6 pracovníků 24 hodin)	28 800,-Kč	
Náklady mzdové správců a bezpečnostních pracovníků (4+4; 24 hod)	38 000,-Kč	
Certifikační náklady ICT	50 000,-Kč	
Celkem:	**2 414 300,-Kč**	

Zdroj: společnost „TELEMUZ s.r.o.“

3.5 Pojem rizika a úspěchu

Riziko[21] v oblasti financování ovlivňuje vedle likvidity a rentability peněžní toky společnosti. Riziko chápeme jako stav – událost, která může za určitých podmínek a s určitou pravděpodobností nastat a mít nějaká dopad na finanční toky společnosti ať ji ž v kladném nebo záporném smyslu. Riziko je vždy spojeno s rozhodováváním o financování projektu (aktiva), zda zdroje společnosti jsou dostatečné nebo je nutné získat zdroje cizí s určitým rizikem.

Bankovní instituce jako zdroj cizího kapitálu pro realizaci záměru mají zpravidla nárok na fixní platby zahrnující úroky a splátky dluhu, bez ohledu jestli záměr je ziskový či není a tudíž úspěch záměru je omezeno splácením závazků. Riziko i úspěch podnikatelského záměru lze rozložit mezi několik investičních subjektů.

3.6 Použité analýzy rizik

3.6.1 Riziko jako stále přítomné nebezpečí

Riziko[10] je definováno jako výskyt nejistoty a nebezpečí v dané situaci s pravděpodobností, že se toto stane či nikoliv. Riziko sebou nese vždy nejistotu, obavy, následky rozhodování, které můžeme rozdělit do objektivního a subjektivního rozhodnutí o dané situaci.

3.6.2 Identifikace, řízení, vyhodnocování rizik

Identifikace a řízení rizik a jejich následků je dlouhodobý, nekonečný boj s definováním vlastní strategie obrany a hlavně útokům proti těmto rizikům. V každém podnikatelském záměru je nutné rizika definovat, následně přijmout ochranné a obranné strategie a získat konkurenční výhodu nad těmito riziky. Každá oblast podnikání má specifický soubor rizik podnikání. Mezi základní patří konkurence, finanční krytí projektu, návratnost investice a maximalizace zisku s minimálními náklady.

3.6.3 SLEPT analýza

Analýza SLEPT je založena na analyzování okolí společnosti a jejich dopadů na sledovanou společnost:

- Social – sociální hledisko – skladba a počet obyvatel, populační politika, kvalifikace, prostředí, etika;
- Legal – právní a legislativní hledisko – podnikání vymezeno zákony, vyhláškami, nařízeními, které udržuje podnikání na vysoce profesionální výši, při porušení sankce – vymahatelnost práva, exekuce, korupce, kriminalita;
- Economic – ekonomické hledisko – DPH, recese ekonomiky, ekonomická síla žadatelů, poptávka a nabídka trhu;
- Policy – politické hledisko – legislativa, nestabilita a poplatnost silových ministerstev jednotlivým stranám a koalicím, podnikatelské loby, byrokracie;
- Technology – technické hledisko – vědecko-technický rozvoj oboru, bezpečnosti, ekologie, enviromentalní politiky;

Další sledované parametry analýzou SLEPT jsou přírodní a klimatické faktory ovlivňující vize a cíle společnosti v návaznosti na maximalizaci zisku.

3.6.4 PORTER 5 sil „5P“

Analýza „5P“ je analýzou dynamických faktorů rozhodujících o výnosnosti a maximalizaci podnikatelského záměru a strategického myšlení. Investice a KNOW-HOW, každého podnikatele jsou ovlivňovány odvětvím podnikaní, vstupy a výstupy, náklady, investičním záměrem a návratností investice do podnikatelského záměru.

Tabulka č.36: „5P“ analýza

Potencionální noví konkurenti Nabídka od konkurence pod cenovou rentabilitu projektu , odčerpání finančních prostředků společnosti a zadlužení		**Kupující** Výběr je zúžen na instituce, které jsou ze zákona povinni tyto systémy provozovat a jejich finanční náročnost
	Konkurenti v odvětví ICT Intenzita soupeření	
Dodavatelé Nové progresivní technologie pro koncového zákazníka		**Náhradní (nové) služby** Servis, konzultace, řešení incidentů jako nezávislý auditor

Zdroj: vlastní

3.6.5 SWOT analýza

Analýza SWOT je analýzou dynamických faktorů rozhodujících o výnosnosti a maximalizaci podnikatelského záměru a strategického myšlení. Investice a KNOW-HOW, každého podnikatele jsou ovlivňovány odvětvím podnikaní, vstupy a výstupy, náklady, investičním záměrem a návratností investice do podnikatelského záměru.

Tabulka č.37: SWOT analýza

SILNÉ STRÁNKY Dlouholeté zkušenosti v oboru Kvalifikační předpoklady Pozáruční servisní služby Bezpečnostní prověrka Flexibilita poskytovaní služeb Propracovaná strategie firmy Sledování a prezentování inovací v oboru	SLABÉ STRÁNKY Konkurence v oboru Povaha sužby Úzká specializace Dostupnost certifikovaných komponentů Opakování prověrek pracovníků Získání certifikátů NBÚ
PŘÍLEŽITOSTI Malý počet certifikovaných společností takový podnikatelský záměr realizovat Proniknout do sféry státní správa jako stabilní zdroj financí Orientace na kvalitu, specializaci, inovaci Konkurenční výhoda Vybudování stabilního postavení společnosti	HROZBY Hrozící ekonomická krize – recese Zvýšení cenových vstupů do záměru Tlak ze strany zákazníků na porušovaní zákonu, předpisu, nařízení za účelem snížení bezpečnostní politiky Zvýšení nebo výpověď nájemních smluv Nesprávně zvolená marketingová strategie

Zdroj: vlastní

3.6.6 Měření rizik a použití metod při vlastní realizaci

Důležitou etapou práce je stanovení rizik komunikačního a informačního systému a to podle standardu ISO/IEC 270002, který vychází z britské normy BS17799.

Analýza rizik podle norem musí být v součinnosti se stanovením vlastní bezpečnostní politiky systému. Riziko většinou neexistuje izolovaně, ale je to soubor pochybení, řetězec náhod, které se nahromadí v čase a v konkrétním případě. Pravděpodobnost jejich výskytu a zaměření nelze určit, ale vždy se jedná o škodu nebo destrukční činnost proti chráněnému zájmu či společnosti. Cílem analýzy rizik je tyto pochybení stanovit a učinit opatření:

- Srovnání rizik a následných kontrol k odstranění rizik,
- Přístup uživatelů v IS podle odhadu informačních aktivit,
- Pravdivost a věrohodnost informace závisí na mnoha vztazích, jednotka informace je nejistá, neobecná,
- Vyhodnotit hrozby, jaké hrozby hrozí chráněným zájmům,
- Chybná nebo megalomanická navržená opatření k ochraně chráněným zájmům, kdy chybně provedená analýza zvyšuje ekonomické zatížení a investice do systému

Pro měření a vyhodnocování včetně členění rizik lze sestavit druhy rizik, která budou zohledňovat následující:

- Makro a mikro ekonomická rizika;
- Bezpečnostní rizika;
- Úmyslná a neúmyslná rizika;
- Výše škody;
- Determinalistická, stochastická;
- Časová;
- Vnější nebo vnitřní;
- Objekt rizika;

Pro stanovení a vyjádření veličin rizik v komunikačních a informačních systémech lze využít dvě metody k řešení problému a to kvantitativní a kvalitativní nebo jejich kombinací.

Kvalitativní metody se vyznačují tím, že rizika jsou vyjádřena a presentována v rozsahu $<-\infty;+\infty>$, či výskytem pravděpodobnosti $<0;1>$. Výsledek je určován

odhadem. Jedná se o metodu rychlejší, jednodušší, subjektivnější, ale chybí finanční vyjádření s kontrolou efektivností nákladů.

3.6.7 Metoda účelových interview (metoda Delphi)

Nejpoužívanější kvalitativní metoda, která spočívá v řízeném kontaktu mezi experty hodnotící rizika a představiteli hodnoceného subjektu, pomocí souborů otázek, prodiskutovávaných na účelových pohovorech. Výsledek obvykle určuje, co se může stát a za jakých podmínek.

Kvantitativní metody se vyznačují tím, že rizika jsou vyjádřena matematicko-statistickými metodami, výpočtem rizika z frekvence výskytu hrozeb a jejího dopadu. Jedná se o metodu výpočtu předpokládané roční ztráty (ALE) s finančním vyjádřením. Metoda je exaktnější, zdlouhavější, složitější, s finančním vyjádřením rizik a s kontrolou vynaložených nákladů. Kvantitativní metodiky jsou ALE, BPA, CRAMM, COBRA, MELISA.

3.6.8 Metoda ALE

Je metoda použitých kvantitativních analýz rizik. V informačních systémech je metoda ALE (Annual Loss Expectancy):

$$SLE * ARO = ALE$$

SLE (Sinngle Loss Expectancy) – hodnota očekávané finanční ztráty pro každý případ uskutečnění bezpečnostní hrozby;

ARO (Annualized Rate of Occurence) – frekvence očekávání uskutečnění hrozby ($^{počet}/_{rok}$),

3.6.9 Metoda BPA

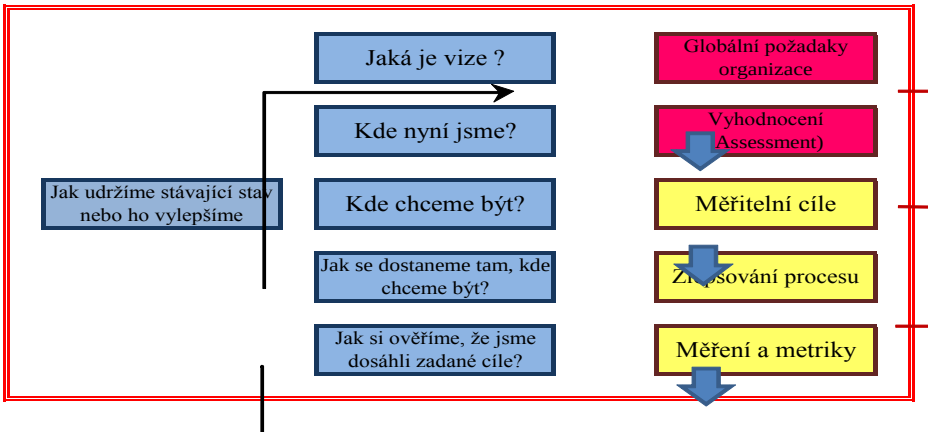
Metoda BPA (Business Process Analysis) je používána v kvantitativní analýze rizik v informačních systémech, používá širší pojetí rizik nejen v informačních systémech, je zaměřena na ekonomická rizika ovlivňující finanční situaci zkoumané jednotky.

3.6.10 Metody CRAMM, COBRA, MELISA

Jsou další metody z používaných kvantitativních analýz rizik v informačních systémech. Analyzují a řeší ohodnocení systémových aktivit, aktivit logických skupin a stanovení hrozeb, zkoumají zranitelnost systému se stanovením bezpečnosti pro jednotlivé skupiny s následným návrhem opatření, které musí být ve shodě s finanční investicí na úrovni rizika a implementovanými systémovými opatřeními.

Součástí metody analýz rizik jsou výstupy a postupy společnosti, kam zaměřit snahy o zvýšení opatření v informačních a komunikačních systémech. Jedním z typických příkladů jak implementovat metody analýzy rizik je následující tabulka:

Tabulka č.38: Metody analýzy rizik



Zdroj: Přeloženo z knihy Planning to implement ITSM ITIL (OGC), Typický postup hodnocení IT procesů

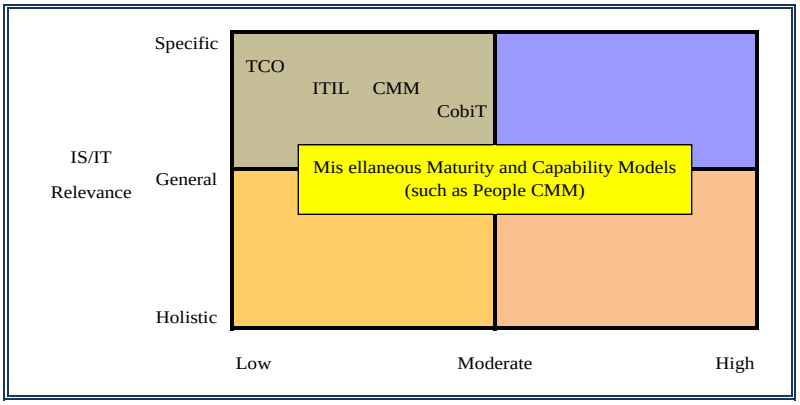
Postupy zavádění analýzy rizik je systém metrik, které jsou zaměřeny na:

- Určení metrik podle cílových skupin;
- Definování zdrojů dat a způsobů jejich získání;
- Vytvoření definice pro výpočet metriky;
- Odsouhlasení časových intervalů měření;
- Určení prahové a cílové hodnoty pro metriky;
- Popsání odpovědnosti managementu v procesů monitorování metrik a kontrolní činnosti;

Při použití analýzy rizik v souběhu s metrikami a jejich vyhodnocením je nutné mít na paměti, že se jedná o:

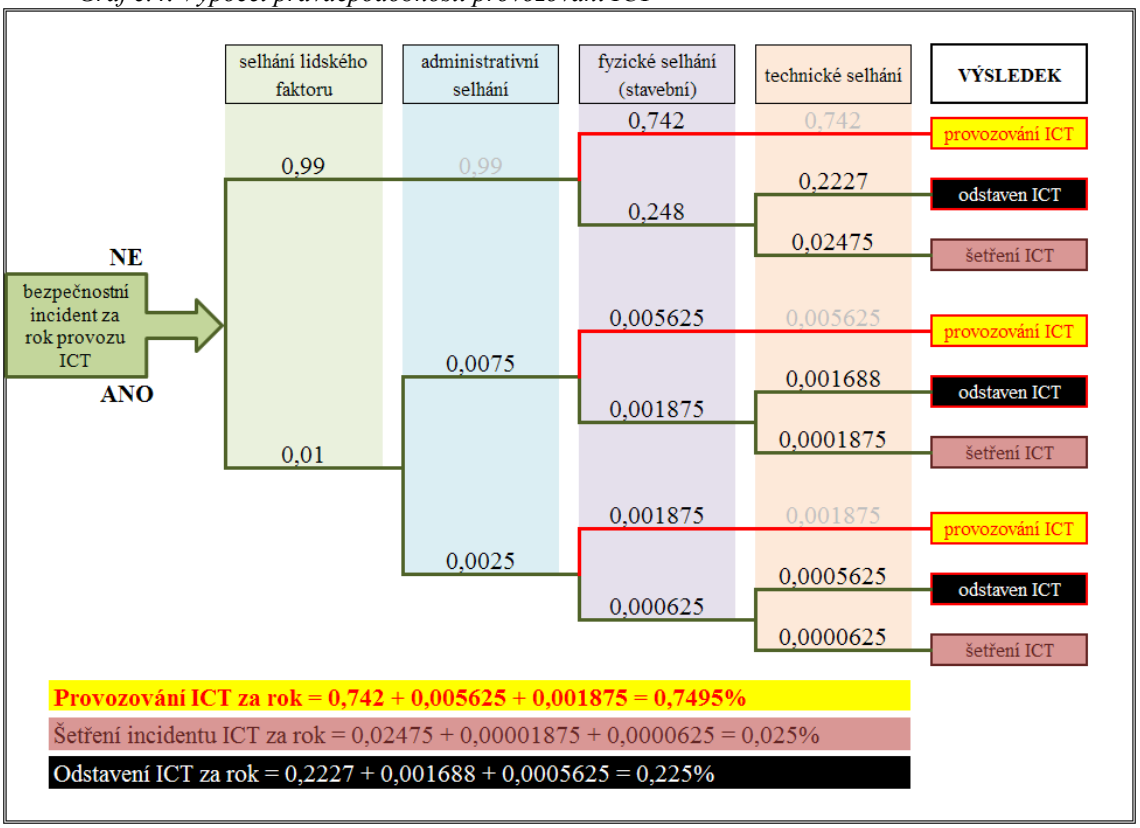
- „Tvrdé“ metriky – hodnocení a kontrolování systémových a síťových nástrojů, databázových dotazů, měření odezvy dotazů, identifikace a jedinečnost uživatele;
- „Měkké“ metriky – hodnocení a kontrolování dotazníky, pohovory, telefonicky;

Tabulka č.39: Metody metrik ICT



Zdroj: IS Proces Improvement: Making Sence of Available Models, Gartner Group, 11 July 2003
TCO – total cost of ownership; ITIL – IT Information Library; CMM – Capability maturity Model; CobiT – Control Objectives Related Technology

Graf č.4: Výpočet pravděpodobnosti provozování ICT



Zdroj: společnost „TELEMUZ s.r.o.“

4 Návrh podnikatelského záměru s ovlivňujícími faktory

4.1 Finanční realizace

S současné době recese ekonomiky, je rozhodnutí investovat do těchto dlouhodobých investic[18],[3],[4], v podstatě do nehmotných komodit, vysoce složitým rozhodnutím, jelikož ochrana dat a informací v okamžiku zavedení nepřináší finanční užitek, ale s délkou používání jeho roste finanční hodnota.

Jak již bylo v předcházejících kapitolách zmíněno, hlavním cílem diplomové práce je vypracovat podnikatelský záměr s navržením, posouzením a teoretickým zhodnocením investice do komunikačního a informačního systému pro státní správu[33]. Tento záměr bude instalován a provozován na úseku ministerstva vnitra a jejich podřízených složek, jako je Policie ČR, HZS ČR, BIS ČR.

Na realizaci podnikatelského záměru [3] je nutné sestavit finanční plán, který by měl pro potenciálního investora rozhodující význam. Musí být zřejmé, že podnikatelský záměr je z finančního hlediska realizovatelný přináší uspokojivou míru výnosu. Při realizací je nutné vytvořit rozpočet, který bude obsahovat:

- Předpokládanou výši nákladů – tato hodnota je stanovena z teoreticko profesní intuitivní zkušenosti pracovníků a managementu společnosti;

Tabulka č.40: Náklady na vybudování a provozování modulu systému

Název činnosti	Náklady zprovoznění	100 Mega	Czech Computer	AutoCont	Auroton
Celkové náklady na hardware na 5 PC	0,-Kč	405 000,-Kč	418 700,-Kč	403 700,-Kč	390 300,-Kč
Celkové náklady na software na 5 PC	0,-Kč	149 500,-Kč	146 400,-Kč	150 000,-Kč	147 500,-Kč
Náklady na krypto od firmy SECUNET	225 000,-Kč	0,-Kč	0,-Kč	0,-Kč	0,-Kč
Celkové technické náklady na vybudování modul ICT pro 5 PC	2 414 300,-Kč	0,-Kč	0,-Kč	0,-Kč	0,-Kč
Celkem návrh:	**2 639 300,-Kč**	**554 500,-Kč**	**565 100,-Kč**	**553 700,-Kč**	**537 800,-Kč**
Reserva 10% z nákladů	263 930, ,-Kč	55 450,-Kč	56 510,-Kč	55 370,-Kč	53.780,-Kč
Celkem návrh:	**2 903 230,-Kč**	**609 950,-Kč**	**621 610,-Kč**	**609 070,-Kč**	**591 580,-Kč**

Zdroj: společnost „TELEMUZ s.r.o.“

Celkové navrhované náklady na komunikační a informační systém na jedno centrální pracoviště a pěti počítačů u uživatelů činí **3 494 810,-Kč**. K této finanční nabídce je nutné přičíst finanční náklady na vybudování komunikačních tras k připojení koncových uživatelů na centrum. Při výběru byla dána výhoda firmám, které dodávají hardware i software a mají certifikát na zařízení proti parazitnímu vyzařování.

- Předpokládanou výši výnosů – tato hodnota je stanovena z pravděpodobnosti výskytu bezpečnostního incidentu a hodnoty chráněného zájmu;
- Předpokládanou výši potřebného kapitálu – tato hodnota je stanovena pro pokrytí podnikatelského záměru investičním a oběžným majetkem, zvážení poměru cizího a vlastního kapitálu, splácení úroků, časové rozložení zatížení, ale využití výhody poskytnutí úvěru bankovními institucemi;

K posouzení finančního krytí podnikatelského záměru společnost se rozhoduje mezi různými druhy[20] financování:

Tabulka č.40: Finanční porovnání mezi vlastními a cizími zdroji pro realizaci záměru

Původ financování / **Právní postavení**	**Vnitřní financování** (podnik se financuje vlastním i silami zevnitř)	**Vnější financování** (do podniku se přivádí cizí kapitál)
Vlastní financování (financování vlastním kapitálem)	Zisky se nevyplácejí investorům vlastního kapitálu (samofinancování)	Zvýšení vlastního kapitálu v podobě peněžních vkladů
Cizí financování (financování cizím kapitálem)	K financování se používají účetní reservy	Přísun cizího kapitálu, např.: leasing, úvěr, dotace

Zdroj: „Podnikatelský plán pro úspěšná start" prof. Dr. Udo Wüpperfeld, str. 109

4.1.1 Leasing

Je jednou ze základních forem financování podnikatelského záměru, jedná se o třístranný vztah ve formě pronájmu HM i NHM a práv, kdy pronajímatel za úplatu nebo jiné nepeněžní plnění nájemci právo danou věc používat. Důležitá je doba pronájmu, cena, ekonomická životnost pronajatého majetku. Základní dělení leasingu[21]:

- Finanční leasing – jedná se o pronájem, kdy po skončení pronájmu dochází k odkupu najaté věci, se smluvní údržbou, opravami a servisem;
- Operativní leasing – jedná se o pronájem, kdy po skončení pronájmu dochází k vrácení najaté věci pronajímateli, kdy údržbou, opravy a servis hradí pronajímatel;

Cena za využití leasingu je cena, která se obvykle platí v pravidelných nejčastěji měsíčních splátkách. Leasingová cena placená nájemcem pronajímateli zahrnuje postupné splátky pořizovací ceny majetku.

Marže je cena pro pronajímatele a na ostatní náklady spojené s pronajatým majetkem (úroky z úvěru, poplatky bance za vedení účtu, správní náklady spojené s leasingem).

Celková výše leasingové ceny je pak dána součtem jednotlivých leasingových splátek, ve které se projeví leasingový koeficient, který udává o kolik je vyšší leasingová cena pronajatého majetku oproti pořizovací ceně majetku, kterou vynaložil pronajímatel. Velikost leasingového koeficientu umožňuje vyhodnotit základní měřítko pro zhodnocení nabídky jednotlivých nabídek leasingových společností. Výpočet leasingového koeficientu provedeme, tak že do čitatele započteme všechno, co v leasingu zaplatíme, a do jmenovatele pořizovací cenu majetku. Hodnotu vyšší než 1 za desetinou čárkou násobíme 100 a vyjde nám o kolik % zaplatíme více za leasing.

4.1.2 Úvěr[18]

V bankovní a podnikatelské praxi se setkáme s celou řadou bankovních produktů, které slouží k rozvoji a podpoře podnikatelských aktivit. Jednou ze základních je úvěr[20],[21]. Úvěrové bankovní produkty směřující ke klientovi umožňují získání peněžního kapitálu. Omezení při poskytnutí úvěru je časové (krátkodobé, střednědobé, dlouhodobé), účel poskytnutí (investiční, provozní), instituce, která úvěr poskytuje (bankovní, obchodní, státní), podle zástavy (lombardní, hypoteční), za předpokladu poskytnutí peněžních prostředků za předem stanovený úrok. Členění úroků podle bankovní instituce jakou převezme záruku:

- Peněžní úvěr – subjekt obdrží formu finančních prostředku a následně je splácí;
- Závazkové úvěry (ručitelské) – kdy bankovní instituce uzavře za klienty závazek plnit závazek vůči třetí osobě;

[18] Malá encyklopedie moderní ekomie, Prof. Sojka, M., Doc. Konečný, B., vydání šesté , 2006 jako svou 371, str. 270 libry®libry.cz, ISBN 80-7277-328-3

Bankovní instituce na finančním trhu poskytují různé druhy úvěrů a jejich kombinací. Mezi nejvýznamnější formy[19] úvěrů patří:

- Kontokorentní úvěr – forma úvěru s pohyblivou výší prostředku a následně je splácí;
- Lombardní úvěry – forma úvěru s fixní výší prostředků s pevně stanovenými pravidly, tento typ úvěru se využívá na financování (cenných papírů, zboží, pohledávek, drahé kovy, pojistky);
- Eskontní úvěr – forma úvěru založena na existenci směnky jako převoditelného cenného papíru;

Splácení úvěru lze realizovat dvěma způsoby:

- Konstantní anuitou (a) – je zadána konstantní úroková sazba = úmor s jednou nebo více splátkami za období (rok);

$$a = D * \frac{\frac{i}{m}}{1 - \frac{1}{\left(1 + \frac{i}{m}\right)^{-n*m}}}$$

- Konstantní úmorem (M) – je zadán konstantní úmor s jednou nebo více splátkami za období (rok);

4.2 Metoda hodnocení efektivnosti investice

Pro podnikatelský záměr a potencionální investory je velice důležité zhodnotit realizovatelnost a dlouhodobou rentabilitu záměru a návratnost vložených investic. K nejpoužívanějším metodám hodnocení výnosnosti investice při věcném investování v praxi současné tržní ekonomiky jsou následující metody statické a dynamické:

4.2.1 Statické metody

- Výpočet rentability – jde o postup, kterým hodnotíme návratnost investovaného kapitálu (poměr očekávaný roční zisk s výší investice);

$$R = \left(\frac{Z}{IN}\right) * 100$$

R – rentabilita investovaného kapitálu (v%)
Z – očekávaný roční čistý zisk

[19] UČETNÍ TEXTY VYASOKÝCH ŠKOL, VUT Brno, FP. PENĚŽNÍ EKONOMIE, Prof. Ing. Rejnuš, O., AKADEMICKÉ NAKLADATELSTVÍ CETRM®, S.R.O. Brno,

IN – investovaný kapitál

- Výpočet návratnosti investice – jde o postup výpočtu doby, za kterou se původní náklady do investice vrátí;

$$N = \left(\frac{IN}{CFr} \right)$$

N – doba splacení investice
IN – investovaný kapitál
CFr – průměrná roční Cash-Flow

4.2.2 Dynamické metody

- Metoda čisté současné hodnoty (Net Prezent Value – NPV) – jde o moderní metodu založenou na matematických postupech, je přesnější, respektuje faktor času pomocí diskontování, Cash-Flow a náklady na investici, zohledňuje velikost, dobu vzniku, délku trvání peněžních příjmů a výdaje během životnost investice;

$$NPV = PV - investice = -C_0 + \sum_{t=1}^{n} \frac{C_t}{(1+r)^t}$$

NPV – čistá současná hodnota investiční varianty
PV – současná hodnota očekávaných výnosů
r – alternativní náklady kapitálu
n – celkový počet let
t– období
C_o– náklady na investici (kapitálový výdaj)

- Metoda vnitřní míry výnosnosti (Internal Rate of rŔetum – IRR) – jde o moderní metodu založenou na zjištění úrokové míry, při které současní hodnota očekávaných výnosů z investice se rovná očekávaným nákladů na investici. Čistá současná hodnota je rovna **nule**.

$$NPV = -C_0 + \frac{C_1}{(1+IRR)^1} + \frac{C_2}{(1+IRR)^2} + \ldots + \frac{C_t}{(1+IRR)^t} = 0$$

NPV – čistá současná hodnota investiční varianty
IRR – vnitřní výnosové procento

5 Zhodnocení podnikatelského záměru

Vlastní zhodnocení a realizace podnikatelského záměru na realizaci komunikačního a informačního systému vychází ze standardů NBÚ a standardů EU, včetně doporučení NATO. Navržený systém je nový, moderní, robustní, komunikační a informační systém, který podporuje manažerské, strategické, ekonomické, bezpečnostní, informační cíle společnosti, chrání citlivá a utajovaná data a informace. Společnosti poskytuje v čase a prostoru konkurenční výhodu při důležitých rozhodováních a získáváni času a finančních prostředků na odvetná opatření skládající se ze zajištění vlastních zdrojů společnosti a cíleného a účinného protiútoku na konkurenci či terorizmus.

Z výsledků ročních uzávěrek za roky 2006 – 2008 vyplývá, že finanční situace firmy „TELEMUZ s.r.o.“ je dobrá. Společnost prochází v současné době personální restrukturalizací a technologickou obměnou zařízení. Společnost na trhu působí od roku 1991.. Společnost má širokou základnu spolehlivých odběratelů, kteří zaručují při správné platební morálce dostatečný a pravidelný přísun finančních prostředků. Společnost sama má dostatek hotovostních finančních prostředků na zajištění potřebné likvidity a hlavně chuť a ochotu přiměřeně riskovat v této oblasti podnikání.

Do současné doby jsem podnikatelský záměr hodnotil z pohledu deterministického a nejpravděpodobnějšího odhadu a dopadu rizik a incidentu s popsáním opatření jak těmto nebezpečím a destrukcím předcházet.

Při realizaci podnikatelské záměru je nedílnou součástí podnikaní riziko, které je spojeno s maximalizací zisků, což je jeden ze základních kamenů podnikání, ale na straně druhé neúspěch – krachu vedoucím ke ztrátám, zadluženosti, likvidaci v nejhorším případě i k lidským a rodinným tragédiím.

Realizace záměru má a musí mít dvě stránky.Stránku pozitivní a negativní. Pozitivní stránky podnikání, pokud pomineme předcházející odstavec o maximalizaci zisku, spojuje podnikatelský záměr s nadějí na úspěch, uplatněním se na konkurenčním trhu, s následným rozvojem společnosti, který přináší zisk, lidské radosti z dobře odvedené práce a zviditelnění na trhu práce a ve společnosti. Negativními stránkami podnikání je zhoršení finanční situace společnosti, zadluženosti, neúspěchu osobního a

kolektivního i přes vynaložení značných finančních, osobních a odborných nákladů. Každý realizovaný podnikatelský záměr je boj nabídky a poptávky na ekonomickém trhu.

I přes tyto skutečnosti popsané v diplomové práci si je společnost „TELEMUZ s.r.o.“ nucena vzít úvěr na uvedený podnikatelský záměr, aby pokryl náklady spojené se zavedením nového, moderního, robustního, komunikačního a informačního systému implementovaného na státní správu. Pod pojmem „ Státní správa[20]“ je nutné si od 1. 1. 2009 představit:

- Organizační složku státu – viz zákon 219/2000 Sb.; s pravomocemi:
    - Organizační složka není právnickou osobou. Tím není dotčena její působnost nebo výkon předmětu činnosti podle zvláštních právních předpisů a její jednání v těchto případech je jednáním státu.
    - Organizační složka je účetní jednotkou, pokud tak stanoví zvláštní právní předpis nebo zákon 219/2000 Sb.
    - Pravidla financování organizačních složek upravují zvláštní právní předpisy,
    - K 31. 12. 2007 bylo v ČR celkem 364 organizačních složek státu
- Ústřední orgány státní správy – zahrnují ministerstva a ústřední orgány státní správy. Konkrétně se jedná o těchto 26 orgánů, které se rozlišují podle toho, zda je v jejich čele člen vlády či nikoliv,
- Další ústřední orgány státní správy – např.: Český statistický úřad, Český báňský úřad, Úřad průmyslového vlastnictví, Úřad pro ochranu hospodářské soutěže, Správa státních hmotných rezerv, Státní úřad pro jadernou bezpečnost, Národní bezpečnostní úřad, Úřad vlády České republiky, Český telekomunikační úřad

Výše získaného úvěru od bankovní instituce bude využita na nákup technologie a potřebných certifikovaných komponentů a na zpracování bezpečnostní politiky.

[20] http://www.czso.cz/csu/redakce.nsf/i/definice_pojmu_ict_ve_verejne_sprave

Tabulka č.42: Celkové náklady na vybudování systému

Název činnosti	Náklady zprovoznění ICT	Náklady na hardware a software	Náklady na jedno PC
Celkové náklady pro 5 PC na prvním objektu	0,-Kč	591 580,-Kč	118 316,-Kč
Celkové náklady pro 5 PC na dalším objektu + kryptografický prostředek	0,-Kč	591 580,-Kč	118 316,-Kč
Celkové technické náklady na vybudování prvního modulu ICT pro 5 PC	2 903 230,-Kč	0,-Kč	698 962,-Kč
Celkové technické náklady na vybudování dalšího objektu pro dalších 5 PC	1 903 230,-Kč	0,-Kč	498 962,-Kč
Celkem návrh:	**4 806 460,-Kč**	**1 183 160,-Kč**	**1 434 556,-Kč**
Celkem:	**5 989 620,-Kč**		
Marže za realizaci záměru:	**33%**	**1 976 575,-Kč**	
Celkem:	**7 966 195,-Kč**		

Zdroj: společnost „TELEMUZ s.r.o.“

Navržený systém je modulový, kde finanční náklady na realizaci jsou vysoce variabilní, náklady na vybudování na základním objektu včetně marže činí 4 648 097,- Kč, celkové náklady na 1 PC včetně marže činí **929 620,-Kč**, které se rozdělí na PC na **772 259,-Kč** za dokumentaci a **157 360,-Kč** na hardware, software a kryptografický prostředek. Další finanční náklady na další budované moduly ICT včetně marže činí **3 318 097,-Kč**, náklady na jedno PC činí včetně marže jen **663 620,-Kč**, které se rozdělí na jedno PC na **506 259,-Kč** za dokumentaci a **157 360,-Kč** na hardware, software a kryptografický prostředek.. Tento rozdíl je způsoben, že zpracovaná bezpečnostní dokumentace je pro celý modulový systém s neomezeným počtem modulů. Každý modul obsahuje 5 PC plně vybavených pro potřeby ICT.

Investice do podnikatelského záměru musí být podložena akceschopným a propracovaným plánem na realizaci, který musí obsahovat časovou, personální, administrativní harmonogram s plnou osobní odpovědností zainteresovaných osob a společností spolupracujících na projektu.

Podnikatelský záměr je nejen nutno naplánovat a finančně zabezpečit, ale zabránit nebezpečí hrozící od konkurence, jak z vnějšího tak vnitřního prostředí.

Podnikatelské lobby neboli konkurence[21], pod tímto pojmem si lze představit volnou soutěž na trhu podnikání mezi podnikateli, usilující získat přízeň zákazníka inovací, příznivou cenou, minimální náklady se zajištěním maximální kvality. Na tomto „podnikatelském poli“ je konkurence minimální, ale zase odborně a technicky vysoce vyspělá. Minimální proto, že před vstupem do těchto podnikatelských aktivit je nutné investovat nemalé finanční prostředky na získání certifikátů od NBÚ, NATO nejen pro společnost, ale i pro zaměstnance. Odbornost a technickou vyspělost musí společnost deklarovat opět na zmíněných úřadech.

Při hodnocení podnikatelského záměru, který chci realizovat pro státní správu se musíme zabývat financováním projektu[22] jako investice. K financování lze použít dva druhy:

- Z vlastních zdrojů za pomocí:
    - Odpisů;
    - Zisku;
    - Výnosu z prodeje a z likvidity hmotného majetku a zásob;
    - Dlouhodobé reservy;
- Z cizích zdrojů za pomocí:
    - Investiční úvěr od bankovního sektoru;
    - Vydáním a prodáním obligací;
    - Splátkovým prodejem;
    - Finančním nebo operativním leasingem;
    - Dlouhodobými úvěry;
    - Státními dotacemi;
    - Dotacemi z EU;

Nejdůležitějším faktorem je rozhodnutí, kolik bude finančních prostředků a z jakých zdrojů je nutné je získat pro realizaci podnikatelského záměru, aby bylo dosažena jeho spolehlivost, včasnost a výše. Státní správa jako vrcholný orgán České republiky a garant všeho makroekonomické dění, musí při uzavření zakázky na bezpečná komunikační a informační systém mít ve svém rozpočtu vyčleněny a

[21] http://www.cepin.cz/cze/clanek.php?ID=41; http://www.petrmach.cz/cze/prispevek.php?ID=43
[22] [22] http://kvf.vse.cz/storage/1180451397_sb_grun.pdf

garantovány finanční prostředky v dostatečné výši. V současné době jsou zakázky pro státní správu nejlukrativnější, nejekonomičtější a nespolehlivější zakázky na trhu práce.

Cizí zdroje financování tvoří významnou část financování investičních záměrů, jelikož tyto zdroje bývají lacinější než zdroje vlastní, na tyto typy zdrojů působí již zmínění finanční páka (cizí kapitál zvedá výnosnost vlastního kapitálu) a daňový efekt (úroky z cizího kapitálu jsou daňově uznatelné). Všechny využité cizí zdroje je nutné splatit, což znamená, že investice musí vydělat na splacení cizích tak, i vlastních zdrojů.

5.1 Financování záměru

Pro financování podnikatelského záměru jsem se rozhodl pro následující variantu:

- 50% hodnoty nákladů úvěrem (4 mil. Kč),
    - Úroková sazba 8% p.a.,
    - Krátkodobý úvěr splatná do 1.roku,
    - Splácení konstantní anuitou nebo konstantní jistinou

Tabulka č.42: Porovnání úvěrů

Porovnání hypotečního úvěru s úvěrem rovnoměrně splácejícím jistinu

Vstupy	Poskytnutý úvěr	4 000 000	Kč
	Úroková sazba	8%	p.a.
	Úvěr poskytnutý na	1	let
	Bud.hodnota	0	Kč
	Typ	0	polhůtní = 0
	Počet splátek	12	

Výstup - hypoteční úvěr

Anuita - měs. splátka **-347 953,72**

Pořadí platby	Úmor	Úrok	CELKEM
1	-321 287,05 Kč	-26 666,67 Kč	-347 953,72 Kč
2	-323 428,96 Kč	-24 524,75 Kč	-347 953,72 Kč
3	-325 585,16 Kč	-22 368,56 Kč	-347 953,72 Kč
4	-327 755,72 Kč	-20 197,99 Kč	-347 953,72 Kč
5	-329 940,76 Kč	-18 012,95 Kč	-347 953,72 Kč
6	-332 140,37 Kč	-15 813,35 Kč	-347 953,72 Kč
7	-334 354,64 Kč	-13 599,08 Kč	-347 953,72 Kč
8	-336 583,67 Kč	-11 370,05 Kč	-347 953,72 Kč
9	-338 827,56 Kč	-9 126,16 Kč	-347 953,72 Kč
10	-341 086,41 Kč	-6 867,31 Kč	-347 953,72 Kč
11	-343 360,32 Kč	-4 593,40 Kč	-347 953,72 Kč
12	-345 649,39 Kč	-2 304,33 Kč	-347 953,72 Kč
CELKEM	-4 000 000,00 Kč	-175 444,60 Kč	-4 175 444,60 Kč

Výstup - pravidelné splácení jistiny

Údaje na konci období po zaplacení splátky i úroku

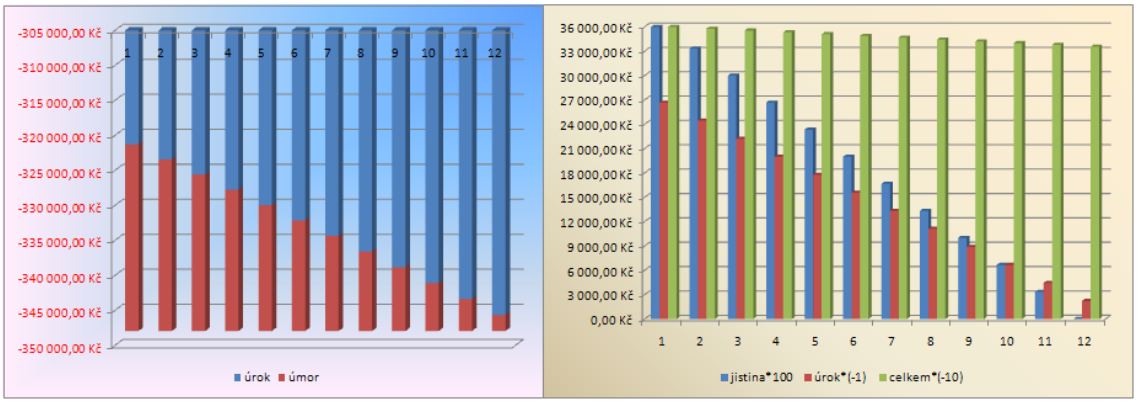
Měsíční splátka	Jistina na konci období	Výpočet úroku *)	CELKEM
-333 333,33	3 666 666,67 Kč	-26 666,67 Kč	-360 000,00 Kč
-333 333,33	3 333 333,33 Kč	-24 444,44 Kč	-357 777,78 Kč
-333 333,33	3 000 000,00 Kč	-22 222,22 Kč	-355 555,56 Kč
-333 333,33	2 666 666,67 Kč	-20 000,00 Kč	-353 333,33 Kč
-333 333,33	2 333 333,33 Kč	-17 777,78 Kč	-351 111,11 Kč
-333 333,33	2 000 000,00 Kč	-15 555,56 Kč	-348 888,89 Kč
-333 333,33	1 666 666,67 Kč	-13 333,33 Kč	-346 666,67 Kč
-333 333,33	1 333 333,33 Kč	-11 111,11 Kč	-344 444,44 Kč
-333 333,33	1 000 000,00 Kč	-8 888,89 Kč	-342 222,22 Kč
-333 333,33	666 666,67 Kč	-6 666,67 Kč	-340 000,00 Kč
-333 333,33	333 333,33 Kč	-4 444,44 Kč	-337 777,78 Kč
-333 333,33	0,00 Kč	-2 222,22 Kč	-335 555,56 Kč
-4 000 000,00		-173 333,33 Kč	-4 173 333,33 Kč

Zdroj: společnost „TELEMUZ s.r.o.“

Při financování podnikatelského záměru úvěrem lze se rozhodnout mezi dvěma variantami splácení a to konstantní anuitou nebo pravidelné splácení jistiny. Z tabulky

vychází rozhodnutí pro variantu pravidelné splácení jistiny, které je výhodnější o **2 111,27Kč**.

Graf č.5: Porovnání úvěrů



Zdroj: společnost „TELEMUZ s.r.o.“

Obrázek č.9: Kalkulačka pro výpočet úvěru

Výše úvěru (Kč)	4000000
Úroková sazba (v %)	8
Délka úvěru v letech	1

Spočítej

Výsledky

Měsíční splátka (Kč)	347953.72
Celkem zaplatíte (Kč)	4175444.60

Zdroj: http://www.mesec.cz/pujcky/hypoteky/kalkulacky/jaka-bude-vase-splatka-hypotecniho-uveru/

5.2 Platební podmínky:

Platební podmínky podnikatelského záměru je nutno stanovit a uzavřít ve smlouvě vždy před uzavřením kontraktu takto:

- 25% hodnoty na začátku podnikatelského záměru,
- 50% hodnoty při dodání technologie podnikatelského záměru,
- 25% hodnoty po dodání technologie podnikatelského záměru,

5.3 Příklad řešení, využití a zhodnocení informace

V současné době státní správa ze zákona zajišťuje transport finančních prostředků mezi tiskárnou státních cenin a ČNB za pomocí silových ministerstev. Tyto informace jsou minimálně pro stát a bankovní instituce, ale i pro subjekty, které podnikají mimo zákon velice citlivé, důležité a v případě zneužití bezpečnostního incidentu - vyzrazením jde o vysoce choulostivou situaci, vysoké riziko zneužití.

Při stávající řešení situace je poměr využití komunikačních a informačních systémů a lidského faktoru jako zdroje rizik v poměru $^{1}/_{3}$: $^{2}/_{3}$, kdy standardní postup je přibližně následujíc s finančním ohodnocen jednotlivých operací:

Tabulka č.44: Porovnání nákladů na akci státní správy

STÁVAJÍCÍ ŘEŠENÍ KOMUNIKAČNÍHO A INFORMAČNÍHO TOKU INFORMACE

STÁVAJÍCÍ NÁKLADY TISKÁRNY STÁTNÍCH CENIN k ČNB

	zpracování dokumentu	počet osob/ks	počet hodin	hrubá hodinová mzda	celkem Kč	CELKEM
Náklady stávající řešení	referenti	2	1,5	200,00 Kč	600,00 Kč	2 300,00 Kč
	kurýrní [illegible]	2	2	150,00 Kč	600,00 Kč	
	využití motorového vozidla	1	1	600,00 Kč	600,00 Kč	
	taxa bezpečnostní politiky	1	1	500,00 Kč	500,00 Kč	

STÁVAJÍCÍ NÁKLADY ČNB ke STÁTNÍ SPRÁVĚ

	zpracování dokumentu	počet osob/ks	počet hodin	hrubá hodinová mzda	celkem Kč	CELKEM
Náklady stávající řešení	ředitel	1	0,5	1 500,00 Kč	750,00 Kč	3 450,00 Kč
	referenti	2	1	200,00 Kč	400,00 Kč	
	kurýrní [illegible]	2	2	150,00 Kč	600,00 Kč	
	využití motorového vozidla	1,00 Kč	2,00 Kč	600,00 Kč	1 200,00 Kč	
	taxa bezpečnostní politiky	1,00 Kč	1,00 Kč	500,00 Kč	500,00 Kč	

CELKEM NÁKLAD
5 750,00 Kč

NAVRHOVANÉ ŘEŠENÍ KOMUNIKAČNÍHO A INFORMAČNÍHO TOKU INFORMACE

STÁVAJÍCÍ NÁKLADY TISKÁRNY STÁTNÍCH CENIN k ČNB

	zpracování dokumentu	počet osob/ks	počet hodin	hrubá hodinová	celkem Kč	CELKEM
Náklady navrhovaného řešení	referenti	1	0,5	200,00 Kč	100,00 Kč	150,00 Kč
	kurýrní služby	0	0	- Kč	- Kč	
	využití motorového vozidla	0	0	- Kč	- Kč	
	využití ICT systému	1	0,1	500,00 Kč	50,00 Kč	

STÁVAJÍCÍ NÁKLADY ČNB ke STÁTNÍ SPRÁVĚ

	zpracování dokumentu	počet osob/ks	počet hodin	hrubá hodinová	celkem Kč	CELKEM
Náklady navrhovaného řešení	ředitel	1	0,3	1 500,00 Kč	450,00 Kč	700,00 Kč
	referenti	1	1	200,00 Kč	200,00 Kč	
	kurýrní služby				- Kč	
	využití motorového vozidla				- Kč	
	využití ICT systému	1	0,10 Kč	500,00 Kč	50,00 Kč	

CELKEM NÁKLAD
850,00 Kč

ÚSPORY NA AKCI
4 900,00 Kč

ÚSPORY NA AKCI ZA ROK
117 600,00 Kč

24

Zdroj: www: MVCR.cz

Při navrhovaném řešení situace je poměr využití komunikačních a informačních systémů a lidského faktoru jako zdroje rizik obrátí v poměru $^{2}/_{3}$:$^{1}/_{3}$.

Toto je jeden z mnoha jednodušších případů využití moderního komunikačního a informačního systému, pro potřeby státní správy, kdy úspora na jeden transport činí **4 900,-Kč** a pokud je proveden 2 krát do měsíce, což je 24 krát za rok, je již úspora ve statisících cca **117 600,-Kč**. Přesná finanční úspora nelze k citlivosti případu zveřejňovat. Takto bychom mohli od jednodušších operací ve finančním světě, přes

rizikové sportovní akce, bezpečností operace, vojenské operace až ochranou před terorismem a extremismem. V celém případu není zohledněna hodnota času, rychlosti, důvěryhodnosti a bezpečnosti. Toto jsou paramenty nevyčíslitelné a empiricky měřitelné.

Použitím nového komunikačního a informačního systému dochází nejen k úspoře financích prostředků, ale snížení rizika získání informace a dat nepovolanými osobami, které by měli zájem o ochráněný objekt a jeho následná ochrana by si opět vyžádala nové finanční prostředky a tudíž základní pravidlo ochrany informací a dat proti zneužití je maximalizace digitalizace dokumentu a elektronický přenos bezpečným systémem od zadavatele až po konečného příjemce. Teoreticky lze vypočítat úsporu např. za 10 let při 15% zvyšování nákladů na ochranu:

$$BH_A = 117600 * \frac{(+0{,}15)^{10} - 1}{0{,}15} = 117600 * 20{,}304 = 2387717{,}30 Kč$$

Předpokládejme, že tuto částku nemusíme čerpat ze státního rozpočtu, při dosažení maximální bezpečnosti a rychlosti zpracovaných dat a informací.

Při zjišťování bezpečnostní incidentů úniku citlivých a utajovaných informací mimo okruh povolaných osob pro zpracování, seznámení a archivaci je největší riziko v lidském faktoru, který úmyslně nebo neúmyslně tento incident spustí a následuje řada neodvratných událostí. Statisticky je dokázáno, že tento incident je v 80% všech úniků dat.

Navrhovaný systém minimálně v 50% eliminuje přístup lidského faktoru jako zdroje rizika k chráněným informacím a datům.

Toto omezení rizika je prakticky nevyčíslitelní a finančně neocenitelné, u každého subjektu je hodnota informace v čase, prostoru a okolí různě ocenitelná k hodnotě chráněného zájmu.

6 Závěr

Základním krokem a prvkem je rozhodnutí stát se OSVČ. Se založením a s realizací podnikatelského subjektu souvisí řada, otázek v celém spektru životaschopnosti zainteresovaných osob, jejich rodin, přátel a hlavně odpovědné ekonomické zajištění osob blízkých. Podnikání je poměrně náročná procedura, která je spojena s určitou mírou rizika, při které je nutné si uvědomit, že riziko je všude přítomné, nepodcenitelné a musí být řiditelné. Je nutné si uvědomit, že i přes počáteční neúspěch v podnikání, lze výrazně snížit a eliminovat rizika získáním důležitých, aktuálních, pravdivých informací, které tvoří základ konkurenční výhody.

Základní okolnosti rozhodnutí je volba právní formy podnikání, která rozhodujícím způsobem ovlivňuje aspekty a formy životaschopnosti podniku v celém aktivním podnikatelském životě, jako je forma živnosti, typ obchodní společnosti, počet zakladatelů, počáteční vklad, administrativa, účast na zisku, daňové zatížení, řídící a rozhodovací pravomoci a jiné zákonné náležitosti dané současným právním řádem.

Kdo založí vlastní firmu projde dlouhou a složitou cestou administrativních, právních a technických jednání kde na konci je společnost, která by měla prosperovat, tvořit zisk pro majitele a podílet se na hrubém národním produktu společnosti. Podnikatelský záměr, jeho realizace a další podnikatelské aktivity jsou poměrně náročné, dlouhodobé a finančně náročné činnosti, spojené se získávání vlastních finančních zdrojů nebo cizích finančních zdrojů od legálních bankovních institucí.

Podnikatelský záměr se musí opírat o plánování na různých stupních a druzích managementu, jehož výstupem je rozhodnutí o realizačním procesu, který stanoví cíle podnikání, způsob jak má být těchto cílů dosaženo, ziskovost projektu, likvidita, riziko spojené s projektem a plánování finančních toku do projektu, které se opírají o účetnictví firmy za uplynulé období, vývoj majetku a způsob jeho financování, druh a výše kapitálu a jejich poměr CK k VK, jeho udržování a rozšiřování.

Cílem diplomové práce je vytvořit podnikatelský záměr na vybudování bezpečného komunikačního a informačního systému, zpracovávající datové, hlasové informace za pomocí kryptografických prostředků v reálném čase a prostředí. Podnikatelský záměr teoreticky zpracovává problematiku komunikačních a

informačních systému ve státní správě, která jako garant bezpečnosti občanů a všech komodit je povinna chránit a ochránit život, zdraví a majetek občanů.

Obecná kalkulace návratnosti investicí do komunikačních a informačních technologií je obtížná a vlastní odpověď ještě před realizací systému v podstatě nemožná. Softwarová architektura představuje bazální investici, kterou společnost musejí naložit jako předpoklad toho, aby v budoucnu vůbec nějaké návratnosti docílila. Existuj veliký počet modelů, zralostí, odborných knih a časopisů, než aby bylo možno říci, že právě tento ztrojme ten pravý. Záleží na konkrétní situaci, potřebách a možnostech zadavatele. Parametry systému se musí setkat ve vhodný čase, místě, události s odpovídajícími možnostmi zákazníka na ochraně proti incidentům, na kterých se dá pak přesně vyhodnotit hodnota chráněného zájmu. Již pouhá změna načasování nebo změna vstupních veličin může výsledek nasměrovat jinam a hodnoty mohu být podstatně odlišné. Je nesporné, že komunikačních a informačních technologie dnes přestavují optimální postupy vývoje, bezpečnosti, integraci v rozhodovacím a řídícím toku.

Náklady spojené s ochranou a bezpečnostní svrchovaností České republiky nelze jednoduše vyčíslit a finančně ohodnotit. Bezpečnost se dá ohodnotit v okamžiku, kdy začneme poměřovat celkové náklady do bezpečnosti komunikačního a informačního systému s celkovými ztrátami a zisky, ztrátou konkurenční výhody či poškození či smrtí chráněného zájmu.Pak cena informace a dat je nevyčíslitelná.

Při řešení podnikatelského záměru bezpečného komunikačního a informačního systému jsem své úsilí zaměřil do sféry státní správy, kdy za 30 let služby v těchto speciálních podmínkách ochrany informací dříve skutečností, ale prioritně citlivých informací v oblasti hospodářské kriminality.

Navržený podnikatelský záměr na bezpečný komunikační a informační systém s vyhodnocením všech rizik přístupu k bezpečnostním incidentům, rizikům, k bezpečnostní politice, finančnímu riziku projektu, likvidity a návratnosti vložených finančních prostředků, lze doporučit. Lze přijmout podnikatelský záměr se všemi navrhovanými bezpečnostními parametry, včetně bezpečnostní politiky na všech stupních a v celém spektru společnosti, ale v režimu maximální přístupnosti pro

uživatele, maximální bezpečnosti systému a s minimálními, ale efektivními náklady na systém.

Při posuzování podnikatelského záměru byly použity analýzy a standardy určené národními a nadnárodními organizacemi, hodnotící kritéria, včetně metod určení efektivnosti, návratnosti a hodnot různých komponentů systému.

Bezpečností systém jako celek je po stránce bezpečnosti hodnocen jako vysoce a maximálně užitečný. Pro uživatele musí být systém maximálně přístupný pro zpracování informací a dat se všemi technickými vymoženostmi 21. století jako jsou např. identifikační karty, biometrie osoby a jiné bezpečnostní prvky.

Z pohledu financování je nutné kladně vyhodnotit systém modulů, které lze přidávat, a tím snižovat celkové náklady na hodnotu chráněného zájmu se zvyšováním počtu uživatelů, dosažitelnosti v prostoru a čase. Pokud se systém rozšíří minimálně do všech 14 krajů, což je předpokládaný stav tohoto komunikačního a informačního systému, bude ochrana dat a informací splněna.

K potenciálnímu nebezpečí, jak z vnějšího a vnitřního prostředí, musí být systém maximálně odolný, neprorazitelný a nepřístupný a musí monitorovat všechny pokusy o napadení, a na základě těchto incidentů za pomocí controllingu se musí přijímat opatření, které budou snižovat počet napadení, s návrhy na zlepšení a zvýšení prevence u uživatelů s následným snižování nákladů do bezpečnostní politiky systému.

Návratnost systému lze těžko v současné době stanovit, ale předpokládaná doba a zkušenost s provozováním současných systému by měla být stanovena minimálně na 10 let. a to z několika důvodů. Jedním ze základních parametrů je návratnost financí, čím déle se systém na technické úrovni provozuje a není potřeba radikálních finančních opatření, je možno tento systém odpisovat v účetnictví jako uznatelné odpisy, jak v účetnictví tak v daňových úlevách.

Realizaci projektu[23] lze rozdělit na hmotnou a nehmotnou část. Projekt je plán, záměr, úmysl, stavebně-konstrukční nebo organizační řešení. S realizací projektu je nutné vzít v úvahu i projektový přístup snažící se sledovat účel, efektivnost a cíl

[23] http://slovnik-cizich-slov.abz.cz/web.php/slovnik/pismeno/P/stranka/126; http://ivs.econ.muni.cz/docs/stud_mat/tahp.pdf

vynaložených prostředků daňových poplatníků. Mezi hmotné části projektu patří v první řadě finance, připravenost objektová, personální, administrativní, informační a kvalitní lidské zdroje. Nehmotné části projektu jsou psychické a duševní pochody v jednotlivých účastnících projektu, které je nutno na poradách sjednotit do jednoho cíle a záměru. Výstupem je ochota realizovat hmotnou část projektu pro státní správu s následným bezpečnostním efektem.

Základ cílem jmenované společnosti „TELEMUZ s.r.o.“ je navrhnout komunikační a informační systém, které je proveditelný[24] záměru je podložen technickou, ekonomickou a finanční analýzou, podpořen matematickými a statistickými výpočty. Na tuto část projektu navazují výpočty hodnot vzdělání a informace.

Výnos navrženého podnikatelského záměru je odvislý od hodnoty chráněného zájmu, ale náklady na vybudování se daly vypočítat a činili na základní modul včetně bezpečnostní dokumentace **4 648 097,-Kč.** Další moduly, na které již nebude potřeba zpracovávat bezpečnostní dokumentaci činí 3 **318 097,-Kč**.

Složitost podnikatelského záměru je podpořena a doplněna analýzou společnosti „TELEMUZ s.r.o.“ za období 2006 – 2008. Ukazatele likvidity, aktivity, zadluženosti a rentability dopadly podle standardů na střední podnikatelské subjekty. Pokud společnosti „TELEMUZ s.r.o.“ vyjde jejich podnikatelský záměr a realizace bude úspěšná, jejich ukazatele likvidity, aktivity, zadluženosti, rentability a výnosnosti se posunout mezi úspěšné společnosti.

Podnikatelský trh je složitá a nebezpečné propojená soustava dějů, které soustavně působí na každý podnikatelský subjekt, který vstoupí do tohoto „ringu“. Působení rizika na každý podnikatelský subjekt je řízení k riziku podnikání, které je nutno analyzovat a řídit, provádět protiofenzívní opatření, která eliminují rizika. I tato analýza rizik je podstatná při rozhodování podnikatelských aktivit. Marketingovou strategií lze různým formám rizik předejít a při získání hodnotové výhody nad konkurencí se rizika snižují. S rizikem je vždy spojena škoda či újma jak hmotná tak nehmotná na chráněném zájmu. Riziko řešené intuitivně, nesystematicky a

[24] http://ivs.econ.muni.cz/docs/stud_mat/tahp.pdf

nevyhodnocované na výsledcích hospodaření společnosti má vždy destruktivní a zničující následky pro společnost.

Závěrem **lze podnikatelský záměr doporučit** pro realizaci společností „TELEMUZ s.r.o.“. I když návratnost a očekávaný finanční zisk nelze jednoznačně určit, ale v uvedeném záměru převažují morální a bezpečnostní ochranné aspekty. Náklady lze s největší pravděpodobností vyčíslit.

V současném světě kde, vládne finanční krize, obavy z terorismu, hladomor třetích zemí, lokální války, obavy z nemocí (AIDS, různé chřipky) je hodnota včasné informace a přiměřených protiopatření nevyčíslitelná. Každý z nás se dostal ve svém životě do situace, kdyby dal „nevím co“ za informaci, která by pomohla odvrátit hrozící nebezpečí proti chráněnému zájmu.

Podpora úspěšného podnikání v tomto oboru je pravidelné analyzování, monitorování situace na segmentu trhu v komunikačních a bezpečnostních systémech, inovace a vědecko-technický rozvoj kryptografických prostředků jako komponentů pro systémy. Do této oblasti patří marketing a management ve všech podobách a stupních společnosti. Taktéž je se vhodné zaměřit na jiný segment podnikání, který bude splňovat představy vedení společnosti „TELEMUZ s.r.o.“.

7 Literatura a zdroje:

7.1 Použitá literatura:

[1] BIGELOW, S. J.: *Mistrovství v počítačových sítích*, překlad Petr Matějů, vydal Computer Press a.s., 2005, ISBN 80-251-0178-9

[2] DOSTÁLEK, L. a KOL.: *Velký průvodce protokoly TCP-IP, Bezpečnost*, vydal Computer Press a.s., 2006, ISBN 80-7226-849-X

[3] FOTR, J., SOUČEK, I.: *Podnikatelský záměr a investiční rozhodování,* vydání první, vydala Grada Publishing, a.s., Praha 2005, ISBN 80-247-0939-2

[4] FOTR, J.: *Podnikatelský plán a investiční rozhodování,* druhé přepracované vydání, vydala Grada Publishing, a.s., Praha 1999, ISBN 80-7169-812-1

[5] GROŠEK, O., PORUBSKÝ, Š.: *Šifrovanie ALGORITMY, METÓDY, PRAX*, vydala Grada Publishing, a.s., 1992, ISBN 80-85424-62-2

[6] HORÁK, J.: *Bezpečnost malých počítačových sítí, praktické rady a návody*, první vydání, vydala Grada Publishing, a.s., ISBN 80-247-0663

[7] KABELOVÁ, A:, DOSTÁLEK, L. a KOL.: *Velký průvodce protokoly TCP-IP a systém DNS*, 3. aktualizované a rozšířené vydání, vydal Computer Press a.s., ISBN 80-7226-675-6

[8] KOCH, M. a spol.: *Informační systémy a technologie*, Skripta VUT Brno FP 1998, str. 7,

[9] Kolektiv: *Informatika pro ekonomy*, Praha, VŠE 1994, Skriptum,

[10] LUŇÁČEK, J., BENEŠ, J.: *Mikroekomonie,* vydání první, vydal VUT Fakulta podnikatelská, 2006 Brno, ISBN 80-214-3293-4

[11] *Microsoft® Windows 98 Resource Kit 1 + 2. díl*, vydal Computer Press a.s., překlad Jiří Hudec, Miroslav Šír, Jiří Farkač, Jiří Veselský, Jiří Gree, Martina Vašíková, ISBN 80-7226-102-9

[12] Microsoft Windows 2003 Resource Kit:

- *Zabezpečení systému a sítě Microsoft Windows*, Ben Smith, Brian Komar, Microsoft Security Team, překlad David Krásenský, Anna Richetská , vydala Computer Press, a.s. 2006, vydání první, ISBN 80-251-1260-8
- *Automatizace správy a skriptování Microsoft Windows*, Don Jones, překlad Jan Gregor, Libor Král, vydal Computer Press, a.s. 2006, vydání první, ISBN 80-251-1261-6
- *Zásady skupin Microsoft Windows*, Darren Mar-Elia, Derek Melber, Milliam . Stanek, Microsoft Group Policy Team, překlad Milan daněk, Jan Pupík, vydal Computer Press, a.s. 2006, vydání první, ISBN 80-251-1262-4
- *Sledování a optimalizace výkonu Microsoft Windows*, Mark Friedman, Microsoft Windows Performance Team, překlad Karel Voráček, vydal Computer Press, a.s. 2006, vydání první, ISBN 80-251-1263-2
- *Řešení problémů Microsoft Windows serverem 2003*, Tomy Northrup, Microsoft Windows Team, překlad Jakub Makulaštík, Anna Rychetská, vydal Computer Press, a.s. 2006, vydání první, ISBN 80-251-1264-0
- *Register Microsoft Windows*, Jerry Honeycutt, překlad Veronika Matějů, vydal Computer Press, a.s. 2006, vydání první, ISBN 80-251-1265-9

[13] MLÝNEK, J.: *Zabezpečení obchodních informací,* vydal Computer Press, a.s. 2006, vydání první, ISBN 978-80-251-1511-4

[14] MOLNÁR, Z.: *Moderní metody řízení informačních systémů*, Praha 1992, vydala Grada Publishing, a.s.,

[15] SHANNON, C. E.: *A Mathematical Theory of Communication*, Bell System Technical Journal, v 27, n.4, 1948, pp. 379-432, 623-656;

[16] SHANNON, C. E.: *Communication Theory of Secrecy System*, Bell System Technical Jornal, v 28, n.4, 1949, str. 656-715;

[17] SMEJKAL, V., SOKOL, T., VLČEK, M.: *Počítačové právo,* vydání první – Praha, 1995, ISBN 80-7179-009-5 (C. H. BECK), ISBN 80-7049-101-9 (SEVT), ISBN 3-406-38730-6 (C. H. BECK. München)

[18] SOUKUPOVÁ, J., HOŘEJŠÍ, B., MACÁLOVÁ, L., SOUKUP, J.: *Mikroekonomie,* třetí doplněné vydání, vydal Management Press, Praha 2004, ISBN 80-7261-061-9

[19] *Vnitřní architektura Microsoft Windows, (Microsoft Windows Server 2003, Windows XP a Windows 2000),* Mark E. Russinovich, David A. Solomon, překlad Ivo Fořt, Karel Voráček, vydala Computer Press, a.s. 2006, vydání první, ISBN 80-251-1266-7

[20] WÜPPERFELD, U. & NISEN, F. – HAUF, M.: *Podnikatelská plán pro úspěšný start,* překlad Doc. Ing. Srpová Jitka CSc. – část 3, 4, Ing. Šiman – část 7.1 – 7.6, Ing. Vojík Vladimír – část 7.7, vydání první, vydal Management Press, Praha 2003, ISBN 80-7261-075-9

[21] Zinecker, M.: *Základy financí podniku,* vydalo VUT Brno, Fakulta podnikatelská, tisk FINAL s.r.o. Olomučany, vydání první, ISBN978-80-214-3704-3

7.2 Použité zdroje:

[22] http://www.myacrobatpdf.com/8427/router-security-guidance-activity-of-the-system-and-network-attack-center-snac.html
15.04.200; 18.45 hod
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head profile="http://gmpg.org/xfn/11">
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<meta name="distribution" content="global" />
<meta name="robots" content="follow, all" />
<meta name="language" content="en, sv" />
<title>Router Security Guidance Activity of the System and Network Attack Center (SNAC) Ebooks Download | Acrobat PDF Files</title>

[23] http://www.itgovernance.co.uk/products/31
18.4.2009; 11.35
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN"><html><head>
<META http-equiv="Content-Type" content="text/html; charset=UTF-8">
<base href="http://www.itgovernance.co.uk/">
<title>ISO/IEC 27002 (ISO/IEC 17799:2005) (Hardcopy)</title>
<meta name="keywords" content="iso17799, ISO 17799, 27002, ISO 27002, ">

[24] http://wikipedia.infostar.cz/c/cl/claude_e__shannon.html

5.5.2009; 22.10 hod
<HTML dir="ltr" lang="cs" xml:lang="cs">
<HEAD>
<META content="text/html; charset=utf-8" http-equiv="Content-Type"></META>
<META content="text/css" http-equiv="Content-Style-Type"></META>
<LINK href="/wiki/Claude_Shannon" rel="canonical"></LINK>

[25] https://dspace.upce.cz:8443/handle/10195/32222

20.4.2009; 22.000 hod
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html>
<head>
<title>Digitální knihovna Univerzity Pardubice: Empirické výzkumy hodnoty informace</title>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<meta name="Generator" content="DSpace" />
<link rel="stylesheet" href="/styles.css.jsp" type="text/css" />
<link rel="stylesheet" href="/print.css" media="print" type="text/css" />
<link rel="shortcut icon" href="/favicon.ico" type="image/x-icon"/>

[26] http://kvf.vse.cz/storage/1168948787_sb_urbanek.pdf

[27]http://www.microsoft.com/cze/windowsserversystem/isaserver/default.mspx

dne 12.07.2004; 20.00 hod,

</nobr><nobr><ahref="/cze/windowsserversystem/isaserver/prodinfo/default.mspx">Informac e o produktu</nobr> <h1>Novinky a vylepšení produktu ISA Server 2006</h1> Aktualizováno: 5. září 2006 ISA Server 2006 nabízí následující nové nebo vylepšené funkce: <h5 style="padding-top: 2px">Obsah této stránky</h5><table cellpadding="0" cellspacing="0" border="0" style="margin-top: 7px; margin-bottom: 12px"><tr valign="top"><td><img width="7" height="9" hspace="4" vspace="2" border="0" src="/library/gallery/templates/MNP2.GenericArticle/../MNP2.Common/images/arrow_px_dow n.gif" alt="Vzdálený zabezpečený přístup k interním serverům od společnosti Microsoft"></td><td class="onThisPage">Vzdálený zabezpečený přístup k interním serverům od společnosti Microsoft</td></tr><tr valign="top"><td><img width="7" height="9" hspace="4" vspace="2" border="0" src="/library/gallery/templates/MNP2.GenericArticle/..

[28] http://www.microsoft.com/cze/WindowsServer2003/sbs/upgrade/benefits.mspx
dne 11.07.2008; 22.30,
hodhref="/cze/windowsserver2003/sbs/evaluation/default.mspx">Informace o produktu</nobr> <h1>SBS 2003 R2: Stručný přehled funkcí</h1> Publikováno: 11. července 2006 Systém Small Business Server 2003 R2 (SBS 2003 R2) je nové vydání aktualizace oceněného produktu SBS 2003. V následující tabulce najdete stručný přehled funkcí a výhod systému SBS 2003 R2.

7.3 Zákony schválené parlamentem ČR:

[29] Zákon č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů ze dne 4. dubna 2002

[30] Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti ze dne 21. září 2005

[31] Zákon č. 151/2000 Sb., o telekomunikacích a o změně dalších zákonů ze dne 16. května 2000

[32] Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a změně některých zákonů (autorský zákon) ze dne 7. dubna 2000

[33] Zákon č. 4/1964 Sb., Občanský zákoník

7.4 Podpůrné normy EU:

[34] Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000, o určitých aspektech služeb informační společnosti, zejména elektronického obchodního styku v rámci vnitřního trhu

[35] Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002, o zpracování osobních údajů a ochraně soukromí v odvětví elektronické komunikace, změněna směrnicí Evropského parlamentu a Rady 2006/24/ES ze dne15. března 2006

[36] ISO/IEC[25] 2382-1;1993 – popis datových prvků – data Elements Description url="/NP/NotesPortalCNI.nsf/key/technicka_normalizace~informace_o_normach~e_byznys~ceska_normalizace~popis_datovych_prvku?OpenDocument&Click=" + v;

7.5 Směrnice a vyhlášky vydané orgány státní moci:

[37] Vyhláška č. 523/2005 o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízeních nakládající s utajovanými informacemi a o certifikaci stínících komor ze dne 5. prosince 2005,

[38] Vyhláška č. 524/2005 o zajištění kryptografické ochrany utajovaných informací ze dne 14. prosince 2005,

[39] Vyhláška č. 527/2005 o stanovení vzorů v oblasti personální bezpečnosti a bezpečnostní způsobilosti a o seznamech písemností přikládaných k žádosti o vydání osvědčení fyzické osoby a k žádosti o doklad o bezpečnostní způsobilosti fyzické osoby a o způsobu podání těchto žádostí (vyhláška o personální bezpečnosti) ze dne 14. prosince 2005,

[40] Vyhláška č. 528/2005 o fyzické bezpečnosti a certifikaci technických prostředků, ze dne 14. prosince 2005,

[41] Vyhláška č. 529/2005 o administrativní bezpečnosti a o registrech utajovaných informací ze dne 15. prosince 2005,

[25] ISO/IEC Information technologii = technická komice informační technologie

8 Seznam tabulek

9 Seznam obrázků

10 Seznam grafů

11 Přílohy

11.1 Příloha č. 1: Základní pojmy a názvosloví informační bezpečnosti:

- **Aktivum (Asset)** — aktiva jsou všechny hmotné a nehmotné statky, vše, co má pro majitele informačního systému nějakou hodnotu. Za nejcennější aktiva se požadují především data a informace, jejichž zneužití, ztráta nebo modifikace by organizaci nebo určité osobě způsobily určitou škodu. Aktiva dělíme na hmotná a nehmotná:
    - **Hmotná aktiva** jsou tvořena uživatelskou technologií, především výpočetní technikou (počítače, servery, disková pole), komunikačními technologiemi (strukturovaná kabeláž, aktivní síťové prvky). Hodnotu těchto aktiv lze zpravidla přesně stanovit v závislosti na jejich pořizovací ceně;
    - **Nehmotná aktiva** představují programové vybavení a data. Patří sem především operační systémy, aplikační programy a programové nástroje pro správu a řízení informačního systému. Nejvýznamnější hodnotu nehmotných aktiv představuje datová základna;
- **Autentizace** je ověření identity uživatele;
- **Autorizace** je pověření k určité činnosti dané přístupovými právy a příslušným oprávněním (pracovat s daty, provádět různé úkony, funkce apod.);
- **Bezpečnost (Security)** chápeme jako vlastnost nějakého objektu nebo subjektu (v našem případě informačního systému nebo informační technologie), která určuje stupeň — míru jeho ochrany proti možným škodám (hrozbám). ztrátě, zneužití nebo zničení;
- **Bezpečnostní analýza IS** — také analýza rizik, hrozeb, představuje odbornou analýzu informačního systému s cílem zjistit rizika a navrhnout protiopatření pro maximální zabezpečení zkoumaného IS;
- **Bezpečnostní audit** (z technického pohledu, ve skutečnosti jde o mnohem více) hodnotí úroveň bezpečnosti neinvazivním způsobem. Základem je pasivní sběr informaci o konfiguraci a nastavení zařízení a následné vyhodnocení těchto informací a vyvození závěrů. Audit je prováděn vždy za asistence administrátora;
- **Bezpečnostní funkce a mechanizmy** definují role bezpečnostních prvků v IS a představují způsob, jakým lze dosáhnout požadovaného zabezpečení jednotlivých komponent systému. Současně také prosazují bezpečnostní požadavky;
- **Bezpečnostní incident (útok)** je snaha o průnik, nebo jinou nepovolenou a škodlivou činnost v rámci ohroženého informačního systému využitím zranitelných míst;
- **Bezpečnostní politika** určuje souhrn požadavků, potřeb, pravidel, směrnic, předpisů a zásad, které jsou definovány pro zabezpečení všech prvků IS na všech úrovních přístupu odpovídajících potřebám a možnostem organizace;
- **Citlivá data (Sensitive Data)** jsou data a informace, které vyžadují ochranu, protože existuje určitá pravděpodobnost působení hrozeb. Jsou to tedy data, jejichž neoprávněné použití může nepříznivě ovlivnit činnost jejich majitele, může mu způsobit určitou škodu. V informačních systémech se především

jedná o personální informace, data chráněná podle zákona státním nebo služebním tajemstvím a informace týkající se chodu organizací — finanční agendy, informace o činnosti atd.;

- **Citlivé informace (Sensitive Information)** jsou informace, které odpovědná autorita určila, že se musí chránit, protože jejich neautorizovaná změna, ztráta nebo zničení mohou způsobit škodu. Tato obecnější definice v dnešní době nahrazuje termín „Citlivá data“;
- **Certifikát** je digitální potvrzení totožnosti připojené k digitálnímu podpisu, použitelné pro ověření pravosti podpisu podepsaného uživatele (u certifikační autority);
- **Certifikační autorita** je instituce,vydávající certifikáty k digitálním podpisům na základě ověřených údajů o žadatelích s mírou odpovědnosti vyplývající z požadované úrovně — třídy certifikátu (Class 1-5);
- **Časová značka** je funkce zjištění daného času a jeho pevného uložení do systému. Jedním z příkladů muže být například časová značka ověřující existenci a platnost digitálního podpisu v daném čase;
- **Detekce průniku (Intrusion Detection System)** (zkráceně IDS) je technika pro odhalování neoprávněné. nesprávné, nebo nezvyklé aktivity v počítačové síti. Tyto systémy lze implementovat jako senzory, které neustále sledují veškerý provoz na síti a srovnávají ho s databází známých síťových útoku (network based IDS), a nebo jako systémy, které detekují napadení přímo na sledovaném hostiteli (host based IDS). Systém kontroluje nejen známé útoky, ale je schopen detekovat i takzvané „pre-attack probes“, což jsou kontrolní úkony prováděné útočníkem před zahájením vlastního útoku. V případě zjištění útoků jsou tyto systémy schopny bránit některým typům těchto útoku, informovat správce a v reálném čase překonfigurovat např. firewally tak, aby bránily vedení těchto útoků;
- **Dostupnost** představuje zachování odpovídajícího přístupu (a to i v případě havárie mateřského systému přechodem na záložní systémy) k informacím nebo službám v souladu s příslušným oprávněním (přístupová práva uživatele);
- **Důvěryhodná počítačová báze (Trusted Computing Base)** je to malá a ověřitelná část informačního systému, která zodpovídá za prosazování bezpečnostní politiky daného systému. Je to soubor všech mechanizmů, které tuto bezpečnostní politiku zajišťují;
- **Elektronický podpis** je obdoba písemného podpisu v digitální podobě. (Digitální podpis je speciální případ elektronického podpisu, kdy k ověření původu dochází na bázi šifrování. Digitální podpis je také dále definován jako krátká datová položka pevné délky vytvořená pomocí kryptografické transformace z elektronické zprávy nebo datového souboru a ze soukromého klíče podepisujícího subjektu. Digitální podpis slouží k ověření identity podepisujícího a rovněž stvrzuje, že zpráva nebyla změněna. tzv. ověření integrity zprávy);
- **Expozice (Exposure)** je místo potenciálního poškození nebo ztráty informací či snížení funkčnosti systému. jde o místo vystavené riziku (např. odhalení utajovaných dat, neoprávněná modifikace, odmítnutí přístupu autorizovaného uživatele ...);
- **FRAM** metodika prováděných analýz rizik;

- **Hodnota aktiva (Asset Value)** je to ocenění důležitosti a významu pro vlastníka. Každý chráněný objekt má svoji cenu. Ta je ovšem rozdílná pro majitele a pro útočníka;
- **Hrozba (Threat)** je skutečnost, událost, okolnost osoby, jejichž působením může dojít k poškození, zničení, ke ztrátě důvěry nebo hodnoty aktiva. Hrozba je tedy jakékoliv nebezpečí. známé, reálné, nebo potenciální, související s rozvojem informačních technologií, které ohrožuje informační systém, nebo data v něm obsažená (např. přírodní katastrofa, vlastní zaměstnanec, hacker);
- **Informační systém (Information System)** je soubor technického (hardware) a programového (software) vybavení, záznamových medií, dat a personálu. který organizace používá ke správě svých informací;
- **Informační technologie (Information Technology)** je veškerá technika, která se podílí na zpracování informací a dat. Jedná se především o výpočetní a komunikační techniku a její programové vybavení;
- **Integrita** je vlastnost, která potvrzuje a zaručuje neporušenost dat v průběhu jejich přenosu od zdroje k cíli (integrita bývá také označována jako celistvost)
- **Kontrola přístupu (Content Security)** znamená, kdo a za jakých podmínek muže komunikovat s naší organizací. Content Security se týká jak předmětu komunikace, tak dat jako součástí komunikace. Content Security však čelí více hrozbám. Tyto hrozby mají svůj původ v interních nebo externích sítích a mohou fyzicky zničit podnikovou infrastrukturu, anebo ji nechat nedotčenou a totálně zničit podnikatelské aktivity. Původ těchto hrozeb může být jak náhodný tak záměrný. Content Security systémy jsou schopné kontrolovat přenos nepřátelských Java applets, ActiveX Controls, Vbscripts a provádět Content management, tedy kontrolu obsahu veškeré pošty, jak odchozí tak i příchozí, a provádět ochranu proti nevyžádaným zprávám (SPAMu), poplašným (hoax) zprávám atd.;
- **Kryptografie** zabývá se navrhováním kryptografických algoritmů a způsoby jejich využívání;
- **Kryptoanalýza** zabývá se metodami umožňujícími získat z šifrovaného textu text otevřený (bez znalosti klíče), zkoumá odolnost (bezpečnost) a naopak zranitelnost jednotlivých kryptosystémů;
- **Kryptologie** je vědní disciplínou zahrnující kryptografii i kryptoanalýzu
- **Kryptografický algoritmus (šifrovací algoritmus, kryptosystém, kryptoschéma, méně přesně šifra)** vyjadřuje matematický postup, který přetváří otevřený text do takové podoby, kdy se původní informace stává nečitelnou a obráceně, postup, který přetváří šifrový text do podoby otevřeného textu;
- **Klíč** tímto termínem je označován parametr kryptografického algoritmu (obvykle utajovaný), bezpečnost kryptosystému záleží na bezpečnosti (dešifrovacího) klíče;
- **Otevřený text** jde o řetězec znaků, který bude šifrován;
- **Šifrový (Šifrovaný) text** jde o řetězec znaků, který je výsledkem šifrování;
- **Šifrování** proces, během kterého je použit šifrovací algoritmus;
- **Dešifrování** proces, kdy získáváme otevřený text ze šifrového textu pomocí šifrovacího algoritmu a dešifrovacího) klíče;

- **Bloková šifra** jde o kryptografický algoritmus převádějící otevřený text po blocích (obvykle v délce 64 resp. 128 bitu);
- **Proudová šifra** jde o kryptografický algoritmus, při jehož užití probíhá šifrování po jednotlivých bitech;
- **Symetrická šifra** jde o algoritmus, který pro šifrování i dešifrování používá tentýž klíč;
- **Asymetrická šifra** je kryptografickým algoritmem, který používá dva odlišné klíče. Jeden pro šifrování a jeden pro dešifrování;
- **Veřejný klíč** takto je označován jeden z dvojice klíčů asymetrického šifrovacího algoritmu. Obvykle slouží k šifrování a nemusí být utajován.
- **RSA** Jeden z prvních (1978) kryptosystémů s veřejným klíčem založený na umocňování v modulární aritmetice;
- **Heslo** Řetězec znaků (obvykle v délce 6 - 16 bytů) sloužící k ověření uživatelovy identity (někdy je kratší heslo např. „x7Kl2O“ silnější, než delší „babicka1“ odhalitelné slovníkovým útokem;
- **Hashovaní funkce** Vytvářejí zprávě jedinečný blok (říká se mu hash či digitální otisk (message digest). Jedinečný proto, neboť je (z výpočetního hlediska) prakticky nemožné nalézt druhou (odlišnou) takovou zprávu, která by měla shodný takovýto hash;
- **Narušení bezpečnosti (Security Incident — Security Breach)** je porušení bezpečnostních kontrol informačního systému, kdy je získán přístup k informacím nebo některé části IS způsobem, který narušuje bezpečnostní politiku;
- **Nepopiratelnost** je jistota, že nelze popřít danou činnost vIS. (Například nemožnost popření přijetí či odeslání zprávy);
- **Neodmítnutí zprávy** (má velký význam v armádě, zajišťuje například přijetí rozkazu);
- **Objekt (Object)** je pasivní entita, která může obsahovat a případně zpracovávat libovolné informace. V informačním systému pod pojmem „objekt“ rozumíme především soubor na paměťovém nosiči, segment paměti, blok dat, záznam;
- **Ocenění rizik (Risk Assessment)** je proces vyhodnocení hrozeb, které působí na informační systém. Cílem je definovat úroveň rizika, kterému je systém vystaven a také zjistit, jsou-li bezpečnostní opatření dostatečně účinná, aby byla pravděpodobnost škody snížena na přijatelnou úroveň;
- **Očekávaná roční ztráta (Annual Loss Expectancy)** z pohledu zvládání rizik expertním odhadem definuje očekávanou roční ztrátu. Tato finanční ztráta vznikne absencí požadovaných bezpečnostních opatření. (Jde o jednu z částí analýzy nákladů);
- **Ochrana aktiv** představuje zabezpečení specifikovaných aktiv před působením definovaných hrozeb, tedy rizik;
- **Protiopatření (Countermeasure)** je jakákoliv činnost, technické zařízení, proces, mechanizmus, nebo cokoliv, co chrání informační systém a jeho části (aktiva) před působením konkrétních hrozeb nebo hrozby. Protiopatření může chránit aktiva před působením hrozby úplně, nebo jen zmírňovat její působení a vzniklé škody;

- **Penetrační test** je test, jehož cílem je vyhledat zranitelná místa informačního systému a tato odstranit. Zkoumá zabezpečení metodou pokusu o průnik. Je prováděn vzdáleně — po síti, obvykle bez asistence správce zařízení a u nalezených slabin bývá často součástí testu demonstrace jejich možného zneužití. Aby byl takový test maximálně účinný, měl by být prováděn zkušenými profesionály, kteří jsou trvale v kontaktu s vývojem informačních technologií a s vývojem snah o narušení jejich bezpečnosti. Jinak jsou některá zranitelná místa přehlédnuta a systém zůstává v provozu se sníženou bezpečností. Po provedení penetračních testů jsou navržena opatření. která budou kompenzovat zjištěná ohrožení. Tato opatření mohou zahrnovat širokou škálu zásahů, od pouhé změny konfigurací systémů až po celkovou restrukturalizaci IS;
- **Průnik (Intrusion)** je neautorizované použití nebo zneužití informačního systému;
- **Registrační autorita** je funkce — osoba, která registruje a zpracovává požadavky na vydání certifikátu k digitálnímu podpisu;
- **Riziko (Risk)** je pravděpodobnost s jakou bude daná hodnota (aktivum) zničena, nebo poškozena působením konkrétní hrozby. Působí na slabou stránku této hodnoty. Je to míra ohrožení konkrétního aktiva;
- **Subjekt (Subject)** je aktivní entita (např. uživatel), která způsobuje a také případně ovlivňuje tok informací mezi objekty. Může ovlivňovat i změnu stavu systému (např. systémový proces);
- **Symetrická a asymetrická kryptografie** jde o způsoby šifrování dat za použití šifrovacích algoritmů. Šifrovací klíče využívají buď symetrické šifrování (klíč pro zašifrování i odšifrování je stejný), nebo asymetrické šifrování (klíčový pár, kde jeden klíč — veřejný klíč adresáta, je určen k zašifrování a druhý soukromý — privátní klíč adresáta slouží k dešifrování);
- **Útočník** je osoba, usilující o nepovolaný zásah do informačního systému (průnik), nebo o krádež, zneužití či alespoň poškození dat, nebo celého systému;
- **Zranitelnost (Vulnerability)** je nedostatek, nebo slabina celého bezpečnostního systému nebo jeho části, která může být zneužita hrozbou tak, že dojde k poškození nebo zničení hodnot — aktiv. Každé aktivum je tedy zranitelné a jeho hodnotu ohrožují různé vlivy. V každém informačním systému existují zranitelná místa — prvky, které jsou využitelná pro útočníka k útoku na data, nebo celý systém. Mohou to být slabiny softwaru, aplikace, ale i lidské (úmyslné i neúmyslné) chyby, neznalost, podcenění bezpečnosti;
- **Zvládání rizik (Risk Management)** je to celkový tj.globální proces, pomocí kterého je možné určit, kontrolovat a omezovat vliv nepředvídatelných nepříznivých událostí tedy hrozeb. Obsahuje především analýzu a odhad rizik, analýzu nákladů a výběr, implementaci, testování a provozování (udržování) bezpečnosti;

11.2 Příloha č. 2: Popis volně šiřitelných softwarů a jejich licenční ujednání pro použití v informačních systémech

11.2.1 Freeware

Je nejznámější skupina těchto programů, v principu se jedná o „normální“ komerční program s jediným rozdílem – je zadarmo. Přitom se jedná často o plnohodnotné programy. Pokud se budeme řídit pravidly o používání freewaru, je možné jej používat a nevystavovat se postihu.

11.2.2 Shareware

Je další variantou programů „zdarma“. Jedná se o regulérní, legální a plnohodnotné programy obsahující zkušební dobu, po kterou je možné je zdarma používat. Po vypršení zkušební doby si musí uživatel program koupit nebo odinstalovat. Zde je jasný zákaz tyto programy „crackovat“ či zprovozňovat pokoutně získanými licenčními čísly.

11.2.3 Adware

Je plnohodnotný komerční program, jen se od shareware liší tím, že obsahuje reklamy, pokud si ho koupíte, tato vlastnost zmizí.

11.2.4 Abandonware

Je poslední a asi nejzajímavějších z programů „zadarmo“, nejsou starší pěti let, nikdo je nedistribuuje, neprodává ani nijak oficiálně nepodporuje. Ovšem pozor – zákony u nás ani v zahraničí abandonware neznají a z pohledu práva se jedná o klasické, plně chráněné programy. A to až do okamžiku, kdy se jejich autoři rozhodnou uvolnit je zadarmo jako freeware, nebo do okamžiku, kdy uplyne 70 let od smrti jejich autora. Takže z pohledu práva je abandonware stále plnohodnotný komerční software se všemi právy a povinnosti či šířením.