ZÁPADOČESKÁ UNIVERZITA V PLZNI
FAKULTA ELEKTROTECHNICKÁ

Katedra elektromechaniky a výkonové elektroniky

BAKALÁŘSKÁ PRÁCE

Návrh funkcionality softwaru pro ucelený systém řízení rizik v elektrotechnickém průmyslu

Martin Zozulák **2017**

ZÁPADOČESKÁ UNIVERZITA V PLZNI
Fakulta elektrotechnická
Akademický rok: **2016/2017**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Martin ZOZULÁK**
Osobní číslo:	**E12B0463P**
Studijní program:	**B2644 Aplikovaná elektrotechnika**
Studijní obor:	**Aplikovaná elektrotechnika**
Název tématu:	**Návrh funkcionality softwaru pro ucelený systém řízení rizik v elektrotechnickém průmyslu.**
Zadávající katedra:	**Katedra elektromechaniky a výkonové elektroniky**

Zásady pro vypracování:

1. Popište teoreticky metodiku pro řízení rizik.
2. Vypracujte rešerši v oblasti softwarového řízení rizik (případové studie, odborné články, literatura).
3. Navrhněte ucelený systém pro řízení rizik (funkcionalitu softwaru).

Rozsah grafických prací: **podle doporučení vedoucího**

Rozsah kvalifikační práce: **30 - 40 stran**

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **Smejkal V., Rais K.: Řízení rizik ve firmách a jiných organizacích.**
2. **Korecký M., Trkovský V.: Management rizik projektů se zaměřením na projekty v průmyslových podnicích.**
3. **Bruckner T., Voříšek J., Buchalcevová A., Stanovská I., Chlapek D., Řepa V.,: Tvorba informačních systémů. Principy, metodiky, architektury.**
4. **Elektronické informační zdroje.**

Vedoucí bakalářské práce: **Ing. Jan Šimota**
Katedra technologií a měření

Datum zadání bakalářské práce: **14. října 2016**

Termín odevzdání bakalářské práce: **8. června 2017**

Doc. Ing. Jiří Hammerbauer, Ph.D.
děkan

L.S.

Prof. Ing. Václav Kůs, CSc.
vedoucí katedry

V Plzni dne 14. října 2016

Abstrakt

Předkládaná bakalářská práce je zaměřena na problematiku softwarového řízení rizik a na zjednodušení a zpřesnění dostupných nástrojů na řízení rizik pro malé a střední podniky v elektrotechnickém průmyslu.

Klíčová slova

Riziko, řízení rizik, analýza rizik, software, míra rizika, impakt, pravděpodobnost

Abstract

This bachelor thesis is focused on software risk management and simplification and refinement of available risk management tools for small and medium enterprises in electrical engineering industry.

Key words

Risk, risk management, risk analysis, software, risk measure, impact, probability

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně, s použitím odborné literatury a pramenů uvedených v seznamu, který je součástí této diplomové práce.

Dále prohlašuji, že veškerý software, použitý při řešení této bakalářské práce, je legální.

.....

podpis

V Plzni dne 6.6.2017 Martin Zozulák

Poděkování

Tímto bych rád poděkoval vedoucímu diplomové práce Ing. Janovi Šimotovi za cenné profesionální rady, připomínky a metodické vedení práce.

Obsah

Úvod

Tato bakalářská práce je zaměřena na téma, které se v posledních letech dostává do popředí v oblasti podnikového managementu, a tím je řízení rizik. Význam správného řízení je vysoký, protože usnadní plynulý chod a zajistí vyšší profit společnosti. Dnes se na trhu objevuje velké množství firem, které se zabývají řízením rizik buďto přímo tak, že přebírají rizika a zodpovědnost za jiný podnik, anebo nabízejí a vyvíjí softwarové řešení, které usnadní práci rizikovým manažerům v podniku.

Cílem této práce je návrh jednoduchého a uživatelsky přívětivého systému pro identifikaci, klasifikaci a následné ohodnocení rizik, určeného zejména pro malé a střední podniky. Zaměření na malé a střední podniky (SME – small and medium enterprises) je z důvodu jejich většinového podílu na českém trhu. Konkrétně v České republice podle zprávy Ministerstva průmyslu a obchodu tvořily v roce 2015 malé a střední podniky 99,83 % všech podnikatelských subjektů.[1] Mnoho z nich se zabývá řízením rizik pouze na elementární úrovni nebo se jím nezabývá vůbec. Nejčastějšími důvody jsou složitost celé problematiky řízení rizik, nepřehlednost a cenová náročnost dostupných softwarů, které mají usnadnit řízení rizik v podniku. Z tohoto důvodu je práce zaměřena na rozbor současného nejpoužívanějšího systému hodnocení a řízení rizik, definici jeho slabých míst a návrhu nového, uživatelsky přívětivého systému s cílem budoucí aplikace ve vývoji risk management systému pro SME.

Práce je rozdělena do tří kapitol. První kapitola se zabývá metodikou řízení rizik, kde je teoreticky popsán postup řízení rizika, jeho definice, rozdělení a analýza. Druhá část je zaměřena na softwary určené pro řízení rizik. V této části jsou vybrány a popsány čtyři počítačové programy pro řízení rizik od různých výrobců. Vybrané softwary byly zvoleny tak, aby komplexnost a využitelnost byly vždy odlišné. Třetí a poslední část obsahuje návrh rozšíření základního postupu řízení rizik, u kterého se předpokládá usnadnění a zefektivnění práce rizikovým manažerům.

Seznam symbolů a zkratek

ARM ..... Active Risk Manager

SME ..... Small and medium-sized enterprises (Malé a střední podniky)

ISO ..... International Organization for Standardization

Č*SN* ..... České technické normy

SW ..... Software

1. Metodika řízení rizik

1.1. Definice rizika

Riziko je historický výraz pocházející údajně ze 17. století, kdy se objevil v souvislosti s lodní plavbou. Označoval úskalí, kterému se museli plavci vyhnout. Následně se tím vyjadřovalo „vystavení nepříznivým okolnostem“. Teprve později se objevuje i význam ve smyslu možné ztráty. Dnes již víme, že nebezpečí představuje něco jiného a v teorii rizika souvisí s hrozbou. Podle dnešních výkladů se pojmem riziko obecně rozumí nebezpečí vzniku škody, poškození, ztráty či zničení, případně nezdaru při podnikání. [2]

V dnešní době žijeme ve světě plném nástrah a nebezpečí. Za celý život se nevyhneme riskantním situacím a rizikovým rozhodnutím. Dnes totiž neexistuje činnost, která by neobsahovala jistou míru rizika.

Pojem riziko je definován různě[3]:

- pravděpodobnost či možnost vzniku ztráty, obecně nezdaru
- odchylka skutečných a očekávaných výsledků
- nebezpečí chybného rozhodnutí
- nebezpečí negativní odchylky od cíle (tzv. čisté riziko)
- možnost vzniku ztráty nebo zisku (tzv. spekulativní riziko)
- neurčitost spojená s vývojem hodnoty aktiva (tzv. investiční riziko)

Existuje řada dalších definic rizika. Záleží na oboru nebo odvětví, kterého se týká. Obecně se však všechny shodují v tom, že riziko znamená jistou pravděpodobnost vzniku nenadálé události, která může mít negativní dopad na očekávaný výsledek. Riziko je zjednodušeně určeno pravděpodobností vzniku a jeho závažností.

1.2. Rozdělení rizik

Rizika se dají dělit podle různých zdrojů vzniku. V elektrotechnickém průmyslu je cílem vytvořit výrobek (stroj, elektronické zařízení nebo jeho část, atp.) s co nejmenšími náklady za co nejkratší čas, aby se zvýšil výnos. Během výrobního procesu mohou vzniknout problémy z různých příčin. Rozdíly mezi nimi a jejich důsledky tvoří základ pro různou klasifikaci rizik. Tyto zdroje vzniku se mohou členit na dynamické či statické, spekulativní nebo čisté.[1]

Statická rizika jsou předvídatelná, protože mají tendenci se objevovat s určitým stupněm pravidelnosti. Patří mezi ně například přírodní jevy, nepoctivost jedinců, selhání lidského faktoru. Jejich následkem dojde ke zničení nebo ztrátě majetku. Na rozdíl od dynamických rizik však statická rizika nepředstavují pro společnost přínos.[3]

Dynamická rizika se nedají předvídat, protože je způsobují okolní faktory jako politika, ekonomika, průmysl, konkurence nebo spotřebitelé. Firma tyto faktory nemůže ovlivnit, ale může se jim přizpůsobit či využít nové možnosti ve svůj prospěch.

Dalším častým rozlišením rizik je dělení na rizika čistá a spekulativní. Spekulativní riziko je spojeno s možností zisku stejně jako s možností ztráty. Příkladem může být podnikání nebo hazardní hra. V obou případech je jistá vidina „snadného“ zisku, avšak hrozí zde také možnost ztráty investice nebo vkladu.

Na rozdíl od spekulativních rizik jsou čistá rizika pouze ztrátová nebo nezisková. Čistá rizika se obvykle vztahují ke ztrátám a škodám na majetku organizací a jednotlivců, poškození zdraví, resp. ztrátám na životech jednotlivců a členů organizačních jednotek, vyvolaným přírodními jevy, technickými systémy a jejich selháním a jednáním lidí.[4] Příkladem může být koupě nového osobního automobilu nebo jiného podobného majetku. Nový majitel od začátku riskuje poškození nebo odcizení dané věci. Jinak řečeno riskuje ztrátu nebo žádný zisk. Toto ovšem neplatí, pokud je automobil pořízen za účelem zisku, například podnikatelem, pak se opět jedná o spekulativní riziko spojené se ziskem i se ztrátou.

Další významné dělení je založené na věcné náplni rizik[4]:

- Technicko-technologická
- Výrobní
- Ekonomická
- Tržní
- Finanční
- Legislativní
- Politická
- Environmentální

Technicko-technologická rizika jsou způsobena použitím nové nebo neotestované technologie, výrobních prostředků nebo technických zařízení. Vznikají kvůli neustálému rozvoji a zavádění nových výrobků na trh.

Těchto dělení rizik je nepřeberné množství. Záleží na kritériích, podle kterých jednotlivá dělení vznikají. Pro manažera je podstatné ještě jedno dělení rizik, a to dělení na neovlivnitelná a ovlivnitelná rizika. U neovlivnitelných rizik není možno ovlivnit jejich příčinu (požár, povodeň, ekonomická krize, atp.), ale lze zmírnit vzniklé následky např. pojištěním. Obecně se jedná o vnější rizika, zatímco ovlivnitelná (vnitřní) rizika může manažer snižovat nebo alespoň částečně odstranit.

1.3. Analýza rizik

Při procesu snižování rizik se musí nejdříve začít jejich analýzou, která má za cíl stanovit, v jakém rozsahu mohou tato rizika ovlivnit cíle projektu, a vyhodnotit priority jejich dalšího ošetření.[5] Jinak řečeno analýza definuje hrozby, pravděpodobnost jejich výskytu a závažnosti dopadu na aktiva.

Základní postup při analýze rizik:

1. Identifikace aktiv
2. Stanovení hodnoty aktiv
3. Identifikace hrozeb a slabin
4. Stanovení závažnosti hrozeb a míry zranitelnosti

1.3.1. Základní pojmy analýzy rizik

Nejdříve se určí základní pojmy, se kterými analýza pracuje. Konkrétně se jedná o aktivum, hrozbu, zranitelnost, protiopatření a riziko.

Aktivum je vše, co má nějakou hodnotu. Tato hodnota může být zmenšena působením hrozby. Aktiva se dělí na hmotná a nehmotná. Hmotná jsou například nemovitosti, cenné papíry, peníze, apod. a nehmotná jsou například informace, morálka pracovníků nebo kvalita a kvalifikace personálu. Hodnota je základní charakteristika aktiva, která je objektivně vyjádřena cenou nebo subjektivně ohodnocena podle důležitosti pro vlastníka.

Hrozba může být jakákoliv událost, osoba nebo aktivita, která může způsobit škodu nebo negativně působit na aktiva. Příkladem může být požár, přírodní katastrofa, krádež zařízení, získání přístupu k informacím neoprávněnou osobou, chyba obsluhy, ale i kontrola finančního úřadu nebo růst kurzu české koruny vzhledem k evropské měně.[3] Základní charakteristickou vlastností hrozby je její úroveň.

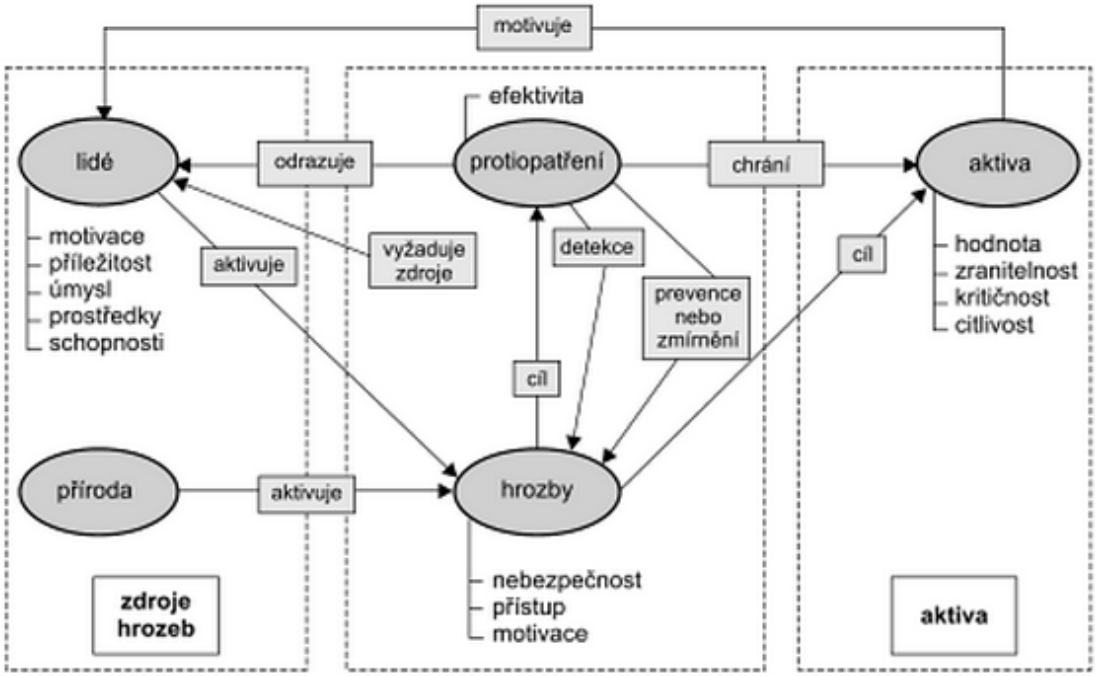
Zranitelností je nedostatek neboli slabina analyzovaného aktiva. Hrozba může využít zranitelnost pro využití svého negativního vlivu. Tato veličina je vlastností, která vyjadřuje, jak je aktivum citlivé na danou hrozbu.

Protiopatření je postup, proces, procedura, technický prostředek nebo cokoliv, co bylo speciálně navrženo pro zmírnění působení hrozby (její eliminaci), snížení zranitelnosti nebo dopadu hrozby.[3] Cílem protiopatření je zabránění vzniku škody nebo usnadnění odstranění vzniklých škod. Protiopatření je charakterizováno efektivitou a náklady.

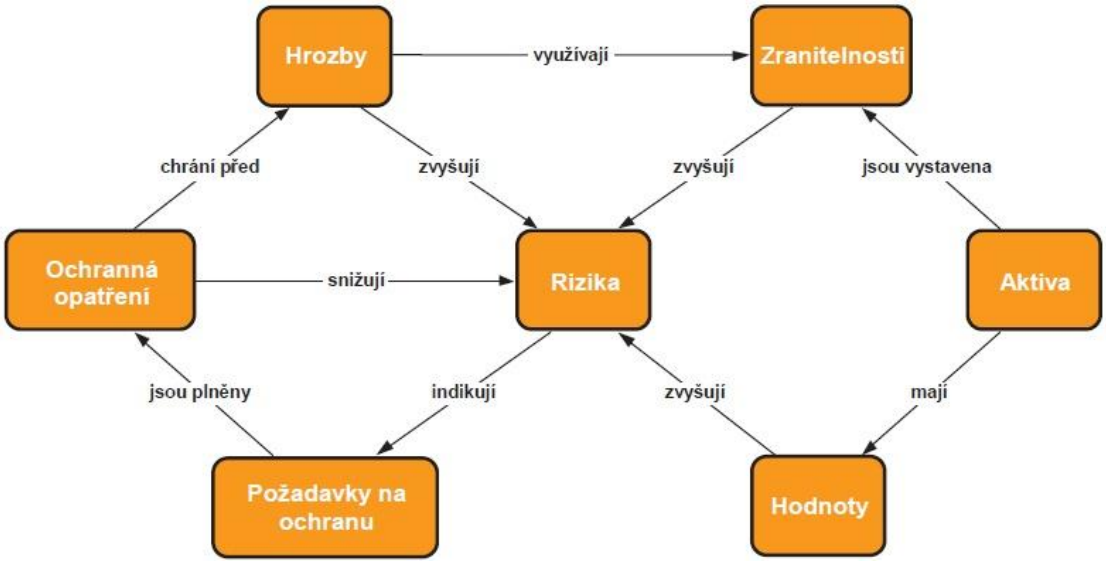
Riziko vzniká vzájemným působením hrozby a aktiva. Protiopatření snižuje úroveň rizika na úroveň, které se říká zbytkové riziko. Velikost zbytkového rizika se porovná s referenční úrovní (tj. úrovní maximálního přijatelného rizika pro subjekt) a podle toho se rozhodne, jestli je nutné podnikat další protiopatření či nikoli.

1.3.2. Vztahy v analýze rizik

Pro úspěšnou analýzu rizik je podstatné uvědomit si, jaké vztahy se vyskytují mezi jednotlivými prvky v analýze. Na obrázku 1 a 2 jsou zobrazeny základní vztahy a souvislosti mezi jednotlivými prvky zmíněnými v kapitole 1.3.1. při analýze a při řízení rizik.



Obrázek 1 - Vztahy a souvislosti v analýze rizik



Obrázek 2 - Vztahy mezi prvky analýzy a řízení rizik

1.3.3. Obecný postup analýzy rizik

Riziko většinou neexistuje izolovaně, ale obvykle se jedná o určité kombinace rizik, které mohou ve svém dopadu představovat hrozbu pro daný subjekt.[3] Protože je množství rizik příliš velké, musí se vybrat nejrizikovější oblasti podle pravděpodobnosti výskytu a velikosti dopadu.

Při analýze rizik se obvykle postupuje v tomto pořadí:

- stanovení hranice analýzy rizik
- identifikace rizik
- stanovení hodnoty a seskupování aktiv
- identifikace hrozeb
- analýza hrozeb a zranitelností
- pravděpodobnost jevu
- měření rizika

Hranice analýzy rizik je fiktivní mez rozdělující aktiva na podstatná, která budou zahrnuta do analýzy, a nepodstatná, která v analýze zahrnuta nebudou. Pro určení této hranice je potřeba znát záměry managementu, případně vypracovat úvodní studii, ze které by bylo možné vycházet. Analýzy se pak budou týkat jen ta aktiva, která jsou pro daný záměr relevantní.

Identifikací aktiv je myšleno vytvoření seznamu všech aktiv, která leží uvnitř hranice analýzy aktiv, přičemž je zadán název aktiva a jeho umístění.

Stanovení hodnoty aktiva se provádí na základě velikosti škody způsobené zničením aktiva. Důležité je určit aktiva jedinečná a aktiva snadno nahraditelná. Z důvodu velkého množství aktiv je potřeba seskupovat aktiva podobných vlastností do skupin.

Pro identifikaci hrozeb lze vycházet ze seznamu hrozeb sestavených podle literatury, vlastních zkušeností nebo průzkumů dříve provedených analýz. Hrozby se mohou odvozovat také od subjektu, jeho statusu (podnikatelský subjekt, orgán státu, nezisková organizace, atd.), postavení na trhu, hospodářských výsledků, záměrů podnikatele.[2] Tyto hrozby mohou potencionálně ohrozit alespoň jedno z aktiv.

Analýzou hrozeb a zranitelností se určí úroveň hrozeb vůči jednotlivým aktivům a úroveň zranitelnosti aktiv vůči těmto hrozbám. Faktory určující úroveň hrozby jsou například nebezpečnost hrozby a její schopnost způsobit škodu. Úroveň zranitelnosti je dána citlivostí a kritičností. Tyto úrovně mohou být sníženy realizovanými protiopatřeními.

Pravděpodobnost jevu určuje pravděpodobnost, se kterou zkoumaný jev,

nastane. Abychom mohli počítat s pravděpodobnostmi, musíme určit, zda je analyzovaný jev náhodný či nikoliv, zda patří do určitého intervalu pravděpodobnosti, případně zda jej můžeme vyloučit a jaké jsou jeho pravděpodobnostní charakteristiky.[3]

Měřením rizika určíme velikost daného rizika. Velikost závisí na hodnotě aktiva, úrovni hrozby a míře zranitelnosti.

Hrubý odhad rizika se stanoví podle rovnice:

$$R = P * I$$

kde R je míra rizika, P pravděpodobnost výskytu rizika a I je impakt neboli dopad rizika nebo

$$R = T * A * V$$

kde R je míra rizika, T je pravděpodobnost hrozby, A je hodnota aktiva a V je zranitelnost aktiva.

Riziko dále měříme podle odchylky od požadovaného výsledku. Čím větší je pravděpodobnost hrozby, tím větší je pravděpodobnost odchylky a tím roste pravděpodobnost rizika.

Směrodatná odchylka je dána odmocninou z rozptylu očekávaných změn charakteristiky:

$$\sigma = \sqrt{\sigma^2}$$

Rozptyl je pak dán vztahem:

$$\sigma^2 = \sum_{i=1}^{n} [r_i - E(r)]^2 * P_i$$

kde r_i jsou jednotlivé hodnoty sledované veličiny, *E (r) je* průměrná hodnota sledované veličiny za určité období, *i* jsou jednotlivé stavy systému (např. časové okamžiky sledování charakteristiky), *n* je počet měření sledované charakteristiky a P_i je pravděpodobnost výskytu jednotlivých stavů charakteristiky.

1.4. Metody analýzy rizik

V dnešní době se používají dvě základní metody analýzy rizik. Odlišují se od sebe způsobem vyjádření používaných veličin. Tyto metody jsou kvalitativní a kvantitativní. V některých případech se používá i jejich kombinace.

1.4.1. Kvalitativní metody

Základem těchto metod je stanovení závažnosti daného rizika. Hodnotí se každé riziko zvlášť, a to na stupnici např. od 1 do 10, nebo podle pravděpodobnosti výskytu od 0 do 1. Další způsob hodnocení je slovní (např. malé, střední a velké). Nevýhodou této metody je její subjektivnost, ovšem výhodou je její jednoduchost a rychlost. Nejběžnější kvalitativní metodou je metoda Delphi.

Metoda účelových interview (neboli metoda Delphi) je založena na řízených interview mezi skupinou expertů a zaměstnanci (respektive představiteli hodnoceného rizika). Na těchto pohovorech se probírá soubor předem domluvených otázek složených ze dvou částí, první je pevná, předem daná, a druhá je variabilní, která závisí na průběhu pohovoru a postavení tázaného. Jednotliví respondenti nejsou během pohovorů v kontaktu, čímž se zamezí vzájemnému ovlivňování. Výsledkem metody Delphi je určení, jaké situace mohou vzniknout a za jakých okolností. Metoda Delphi má více možností průběhu, například metodu anketní analýzy, metodu scénářů nebo metodu matic.

1.4.2. Kvantitativní metody

Tyto metody se zakládají na matematickém výpočtu rizika z četnosti hrozeb a míry dopadu hrozby. Výstupem je číselné ohodnocení incidentu i dopadu události. Kvantitativní metody jsou přesnější než kvalitativní, ale časově náročnější a nákladnější. Jejich výhodou jsou přesnější, správnější a spolehlivější výstupní data. Příkladem kvantitativních metod pro počítačové zpracování jsou CRAMM, @RISK, RiskPAC nebo RiskWatch.

CRAMM (CCTA Risk Analysis and Management Methodology) je pravděpodobně nejznámější metodikou, která byla původně vyvinuta pro potřeby vlády Velké Británie, ale v současné době je široce využívána jako uznávaný prostředek pro analýzu rizik v případech, kdy je vyžadováno dodržení normy ČSN ISO/IEC 13335 a mezinárodního standardu ISO/IEC 17799.[2] Analýza v rámci CRAMM řeší ohodnocení systémových aktiv, seskupení aktiv do logických skupin a stanovení hrozeb působících na tyto skupiny, prozkoumání zranitelnosti systému a stanovení požadavků na bezpečnost pro jednotlivé skupiny, na základě čehož jsou navržena bezpečnostní opatření, která jsou vymezena ve shodě s úrovní rizika při porovnání s již implementovanými systémovými opatřeními.[3] Tento systém je velmi drahý a složitý na obsluhu, proto je určen hlavně pro školené analytiky, ne však pro běžné subjekty.

Metodika **@RISK** používá simulační metody Monte Carlo. Zpracovává celý problém ve formě tabulek. Hodnoty, které nejsou jasně definované, se nahradí funkcemi, které určí rozsah hodnot. Monte Carlo je kvantitativní metoda, která udává pravděpodobnostní rozdělení rizik a hrozeb.

Metodika **RiskPAC** je používána pro automatizaci zpracování dotazníků. Nejde o expertní systém, který by sám rozhodoval o úrovni jednotlivých rizik nebo o pravděpodobnostech výskytu hrozeb a rizik. RiskPAC pouze zpracuje dotazníky a výstupem je stanovení jednotlivých rizik.

RiskWatch je program pro automatizaci zpracování výsledků, které se získaly soubory otázek dělenými na různé bezpečnostní oblasti. Vstupem jsou získaná data z jednotlivých oblastí ve formě tabulek nebo simulační metodou Monte Carlo.

1.5. Řízení rizik

Řízení rizik je proces, při němž se subjekt řízení snaží zamezit působení již existujících i budoucích faktorů a navrhuje řešení, která pomáhají eliminovat účinek nežádoucích vlivů a naopak umožňují využít příležitosti působení pozitivních vlivů.[3]

1.5.1. Obecné zákonitosti řízení rizik

Základem každého řízení rizik je analýza jasně definující rizika, která je nezbytné vzít v úvahu. Dalším krokem je rozhodovací proces, vycházející právě z výsledků analýzy. V úvahu se musí vzít také další faktory, které mohou ovlivnit rizika, například faktory ekonomické, technické (např. technický stav strojů, budov atp.), ale i sociální a politické. Následuje vývoj a srovnání možných opatření. Posléze se z těchto opatření vyberou ta, která sníží, případně eliminují existující rizika. Další a pravděpodobně nejnáročnější fází je výběr vhodného řešení. Nejdříve se určí úroveň rizika, dále se stanoví ekonomické náklady jednotlivých opatření pro snížení rizika a také jejich ekonomické přínosy (cost-benefit analysis). V dalším kroku se hodnotí možný dopad na subjekt nebo přínos pro něj a jeho okolí. Na závěr se rozhodne, které opatření na snížení rizika se použije, případně se rozhodne, jestli je nutné toto opatření dále sledovat, pokud je míra nejistoty výsledku stále vysoká. Tato nejistota představuje zbytkové riziko.

Oblast managementu rizik je velmi rozsáhlá a odlišná podle svého zaměření. Hlavní oblasti, ve kterých se mluví o řízení rizik, jsou[3]:

- Přírodní katastrofy a havárie
- Rizika ochrany životního prostředí
- Finanční rizika
- Projektová rizika
- Obchodní rizika
- Technologická rizika
- Technická rizika
- Politická rizika
- Bezpečnostní rizika

1.5.2. Důležité pilíře systému řízení rizik

Pro efektivní funkci managementu rizik je důležité, aby byl v organizaci realizován jako integrovaný systém s jasně a srozumitelně formulovanými cíli, přehlednou strukturou a postupy.

Předpokladem k tomu je, aby byl management rizik vybudován na těchto základních složkách:

- Strategie managementu rizik
- Identifikace procesů, rizik a nežádoucích událostí
- Zvládání rizik
- Monitorování rizik a dopadů
- Dokumentace, komunikace, informace, znalosti
- Optimalizace podnikového systému managementu rizik

Strategie managementu rizik a jasně zformulovaná podniková politika jsou základem správného managementu rizik. Vedení podniku musí mít jasno v tom, která rizika ohrožují chod podniku nebo jeho činnosti, a kdo a jak se bude těmito riziky zabývat. Vstupem do managementu rizik jsou jasně zformulované cíle podniku a výstupem strategický dokument a akční plány pro jednotlivá rizika nebo jejich skupiny. Výstupy musí zahrnovat všechny vyskytující se typy procesů a obsahovat podklady potřebné pro plánování prevence, snižování rizikovosti, snižování následků a pro řízení procesů a jejich

optimalizaci.

Strategie stanoví základní přístupy, principy, kritéria a postupy, jak organizace analyzuje a zvládá rizika a to tak, aby byly pokryty všechny oblasti rizik – provozní (procesní), technologická, finanční, tržní, bezpečnostní, environmentální, zdravotní a lidský faktor.[6] Vychází při tom ze znalosti vnitřních a vnějších rizikových faktorů, jednotlivých podnikových procesů a z konkrétních podmínek či omezení. Dále musí být zohledněny ostatní strategie a cíle organizace. Velmi důležitou součástí strategie musí být definování postupů a metod použitých při analýzách, určování opatření a zavádění změn.

Hlavní součástí **identifikace procesů, rizik a nežádoucích událostí** je analýza rizik. V dnešní době je to častá slabina podnikových managementů a procesy rizikových analýz nefungují tak, jak je potřeba. Dále je zde zahrnuto zpracování seznamu jednotlivých rizikových procesů a faktorů, včetně jejich popisu, určení zdrojů, atp., hodnocení jejich závažnosti z hlediska pravděpodobnosti a nebezpečnosti a na závěr určení, která rizika a v jakém pořadí by měla být předmětem opatření, případně která rizika mají být předmětem další analýzy.[6]

Existuje velké množství systémů na klasifikaci rizik, avšak není žádný, který by se dal považovat za všeobecný a obecně využitelný. Ani podle mezinárodního standardu ISO 31000:2009 Risk management – Principles and guidelines není správné a bezpečné používat pouze jeden univerzální způsob. Každý podnik by si měl zajistit svůj vlastní systém, který bude právě vyhovovat druhu a typu rizik a velikosti podniku. Kromě výše zmíněného standardu ISO 31000:2009 existují i pomocné dokumenty, které pomohou ke správnému chodu systému řízení rizik. ISO Guide 73:2009 Risk management – Vocabulary a IEC/ISO 31010:2009 Risk management – Risk assessment techniques obsahují základní terminologii, zásady, návody a metody hodnocení pro management rizik. Existují i v České Republice v soustavě ČSN: ČSN ISO 31000 Management rizik – Principy a směrnice (01 0351), TNI 01 0350 Management rizik – Slovník (Pokyn 73) (01 0350), ČSN IEC/ISO 31010 Management rizik – Techniky posuzování rizik.[7][8]

Zvládání rizik má za cíl prevenci nežádoucích událostí a zmírňování jejich následků. Tohoto cíle se dosáhne ve třech fázích, a to ve fázi návrhu opatření, plánu implementace a jeho aplikaci. Při návrhu opatření se vybírají preventivní postupy s ohledem na ostatní

procesy a opatření. Důležité je neupínat se pouze k jednomu řešení, ale zvážit i možná alternativní řešení a porovnat jejich efektivnost a náklady. Reálně se využívá kombinace více různých opatření. Plán implementace by měl vždy kromě vlastních opatření a scénářů jejich realizace stanovit, jak budou zajišťovány potřebné zdroje (lidské, finanční, informační, metodické apod.). Specifikovány musí být odpovědnosti příslušných pracovníků a útvarů, resp. vlastníků implementačních procesů.[6] Následně se postupuje podle vytvořeného plánu. Úspěšné zvládnutí rizika závisí na podpoře řídícího managementu (leadership, sponzorství, hodnocení a oceňování lidské práce apod.).

Jsou zde ale i rizika, která se nedají předvídat. Těmi jsou hlavně nehody a havárie. Mají malou pravděpodobnost vzniku, ale velmi vážný dopad. Běžné metody identifikace rizik na tyto situace nefungují. Zabývá se jimi krizové řízení.

Další složkou systému řízení rizik je **monitorování rizik a dopadů**. Výhodnější než jednorázové analýzy rizik je soustavné monitorování jako systémový nástroj podnikového řízení. Výstupem jsou informace o prevenci, průběhu a dopadu nežádoucích událostí. Monitorování rizik a dopadů je složeno z mnoha složek, jako je sledování činnosti lidí, procesů a technologií, aktivit managementu, funkce ochran proti vzniku a rozvoji závad a nehod atd.

Dokumentace, komunikace, informace, znalosti jsou základními prvky v systému řízení rizik. Z každé analýzy nebo každé metody přichází velké množství dat, se kterými se pak dále pracuje. Důležité je tato data zpracovat a zdokumentovat pro budoucí použití. Z těchto dokumentů se management může dále rozvíjet a mohou se stát nepostradatelným zdrojem pro další aktivity. Příkladem mohou být případové studie, které slouží k urychlení a usnadnění budoucího řešení určitých problémů. Každý podnik by měl mít jasně zformulované požadavky na dokumentaci, na postupy sledování, shromažďování, třídění informací i zajišťování dostupnosti informací a znalostí. Podnik musí dbát, aby příslušné dokumenty, protokoly, rozbory a závěry šetření vyhovovaly svému účelu jak obsahem, tak formou. Musí být zavedeny postupy inovací, aby byla neustále udržována jejich aktuálnost.[6] Pro řízení rizik je klíčová aktivní komunikace mezi všemi úrovněmi podnikové hierarchie. Spolehlivý tok podstatných informací je předpoklad pro fungování managementu rizik.

Předmětem komunikace jsou mimo jiné informace o:

- Nastalých událostech
- Bezpečnostních předpisech
- Strategiích, úkolech, instrukcích, postupech
- Výsledcích analýz a monitorování rizik
- Výsledcích auditů, zjištěných nedostatcích
- Posledních trendech, úspěších
- Vyplývajících úkolech, odpovědnostech, pravomocích, potřebných zdrojích atd.

Optimalizace podnikového systému managementu rizik je založena hlavně na jeho soustavném hodnocení, zejména jednotlivých uplatňovaných opatřeních z hlediska jejich efektivity. Výsledky monitorování rizik jsou průběžně používány pro zlepšení systému a postupů managementu rizik. Dalším zdrojem informací jsou zpětné vazby od zaměstnanců, zákazníků nebo partnerů.

2. Programy pro řízení rizik

Řízení rizik se v dnešní době stává stále důležitější součástí správného chodu podniku. Zvyšují se požadavky na bezpečnost, plynulost chodu podniku nebo výroby, aby nevznikaly chyby, poruchy a ztráty, respektive aby bylo nalezeno řešení problému, pokud možno dříve, než k nějakému dojde. To vyžaduje mnoho času, prostředků a lidí, kteří se budou těmito riziky zabývat. Proto se stále častěji využívají softwarové nástroje k řízení rizik, které tento proces urychlují, zjednodušují a zpřehledňují.

2.1. Funkce softwarového řízení rizik

Software pro řízení rizik (anglicky **Risk Management Software**) je podnikový software, který slouží pro řízení rizik, tedy jejich evidenci, ohodnocení, audit, zhodnocení dopadů rizik a případně shodu s požadavky legislativy.[9] Sofistikované systémy jsou dnes schopné obsáhnout potřeby celého podniku. Od řízení výroby a projektu až po samotný prodej. Takovéto softwary mají největší hodnotu, protože evidují veškerá rizika a poskytují jejich úplnou kontrolu.

Základními funkcemi a vlastnostmi softwaru pro řízení rizik jsou:

- Evidence rizik a vytvoření databáze rizik
- Analýza rizik
- Zhodnocení rizik
- Tvorba a řízení opatření k jednotlivým rizikům
- Řízení shody s legislativou
- Mapa odpovědnosti za rizika
- Interní audit

Nevýhodou takto rozsáhlých systémů je jejich složitost a cena. Aby mohl podnik takové softwary využít, potřebuje k tomu kvalifikovaný personál, který s nimi bude umět zacházet. To obnáší různá školení a tím i další výdaje. Další možností je najmutí externí firmy, která zajistí veškeré rizikové řízení v podniku. Dále jsou k dispozici softwary, které nejsou tak sofistikované a umožní uživateli využít jen základní funkce. Mezi tyto funkce patří evidence rizik, jejich ohodnocení a výsledné určení míry rizika. Tyto nástroje jsou levné a jednoduché na ovládání, ale neobsáhnou všechny potřeby na řízení rizik podniku.

2.2. Srovnání vybraných softwarů pro řízení rizik

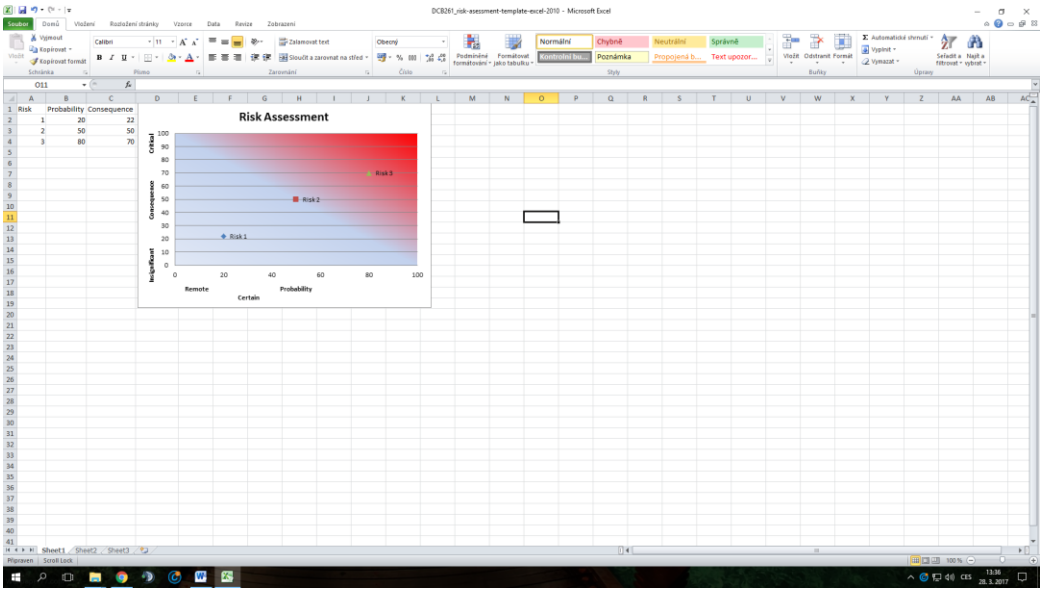
S rozvojem podnikového managementu rizik se rozvíjejí i softwarové nástroje, které se používají. Dnes je k dispozici veliké množství firem a softwarů, které se touto problematikou zabývají. Liší se v různých parametrech a možnostech. Některé jsou určeny pro velké organizace, jiné zas pro menší firmy s určitým zaměřením. Složitější a náročnější softwarové balíky jsou schopné nasimulovat různé situace a tím zpřesnit výsledky jednotlivých rizikových analýz.

Další parametr pro srovnání je cena. Většinu programů lze pořídit za jednotky až desítky tisíc ročně, jiné se zas nedají pořídit jako samostatný software, ale místo toho se najme tým odborníků, který zajistí vše potřebné. Při výběru vždy záleží na potřebách firmy či podniku a na oboru vykonávané činnosti (např. bankovnictví, zdravotnictví, energetika, výroba…).

V této práci jsou vybrány jen některé softwary, které se zabývají řízením rizik. Jsou mezi nimi menší a jednodušší, určené pro malé a střední podniky i velké a rozsáhlé softwarové balíky určené pro velké organizace a společnosti.

2.2.1. MS Excel

MS Excel je zástupce tabulkových procesorů ze softwarového balíku Microsoft Office, který lze použít jako jednoduchý prostředek k výpočtu rizik a následnému grafickému zpracování ve formě grafů či rizikových map. Je dostupný a jednoduchý na používání a pro zkušeného rizikového manažera je dostačující nástroj pro monitorování rizik. Pro nezkušeného uživatele je nevýhoda subjektivnost, protože záleží pouze na uživateli, jak ohodnotí jednotlivá rizika z pohledu pravděpodobnosti a impaktu. Při použití obsáhlejších seznamů rizik hrozí, že grafické výstupy budou nepřehledné a tím i nevhodné pro použití.



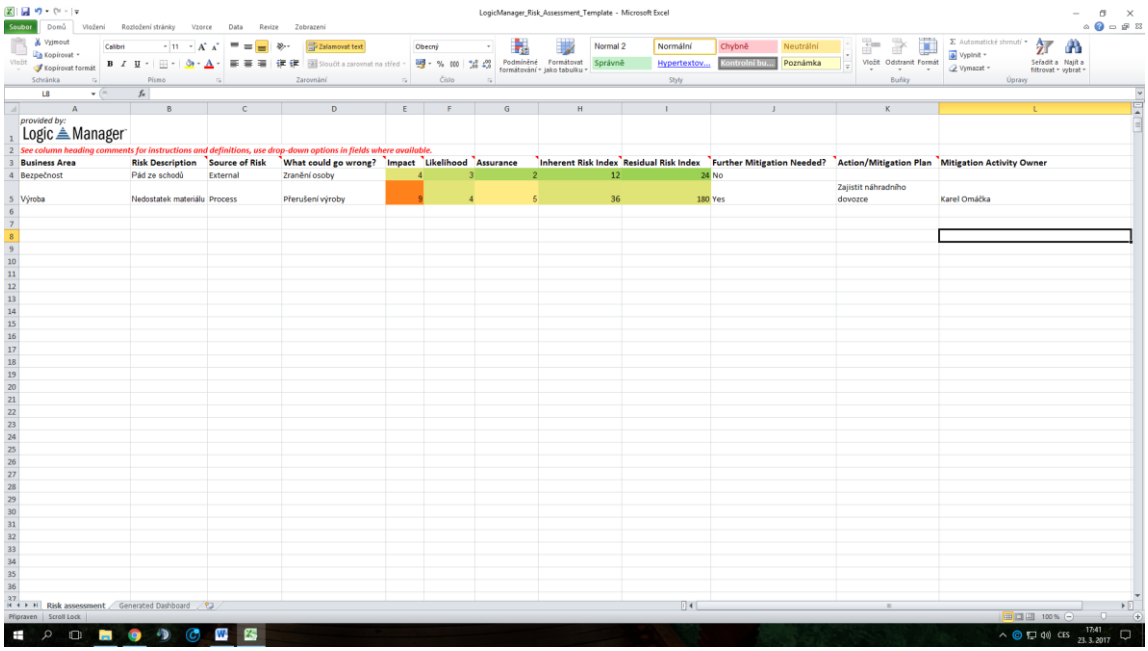
Obrázek 3 - Template pro řízení rizik v MS Excel[10]

2.2.2. LogicManager

LogicManager poskytuje software pro řízení rizik v podniku, který pomáhá rizikovým manažerům snadněji identifikovat, zmírnit a dále pozorovat rizika, která se nacházejí ve společnosti. Umožňuje uživatelům prohlížet existující vztahy mezi riziky s cílem zjistit základní příčiny rizika, a jak ovlivní strategické cíle podniku. LogicManager nabízí různé platformy pro řízení rizik podle potřeb zákazníka a k tomu potřebné poradenství a technickou podporu. Ceny začínají na 6 000 USD za rok, ale záleží na konkrétních specifikách, které cenu upraví. [11]

Tento software je navržen tak, aby automaticky identifikoval redundantní nebo překrývající se činnosti a poskytoval přímé spojení do řízení výkonnosti prostřednictvím přijetí norem, a opětovné použití informací.

Navíc LogicManager poskytuje zdarma k dispozici předlohu pro MS Excel, kterou lze použít jako jednoduchý nástroj pro kalkulaci rizik a jejich řízení. Na obrázku níže je ukázána základní tabulka s již předdefinovanými výpočty, připravená na doplnění o seznam rizik a jejich popis a ohodnocení. Dalším výstupem je mapa rizik podobná té z předchozí kapitoly MS Excel viz Obrázek 4. [11]

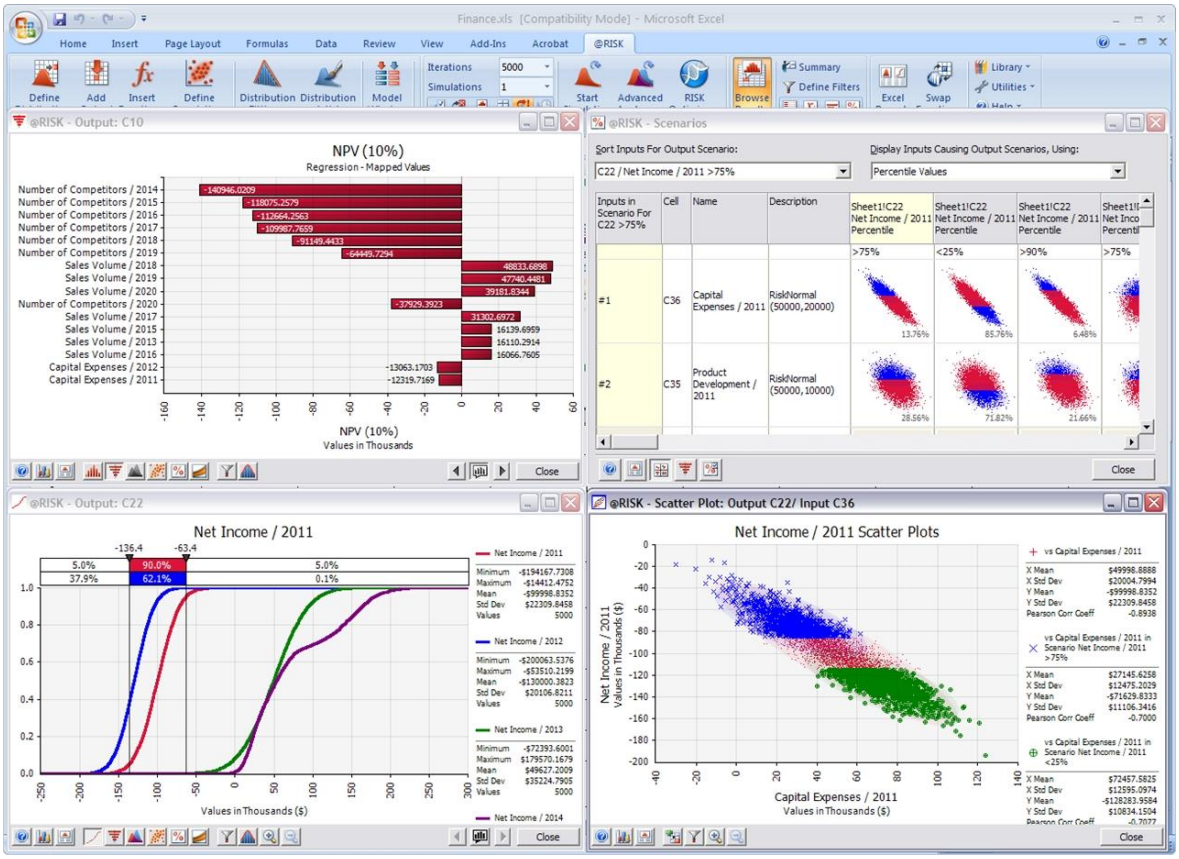


Obrázek 4 - Předloha pro MS Excel od LogicManager[11]

2.2.3. @RISK

Program **@RISK** je profesionálním softwarem od firmy Palisade. Výhodou tohoto programu je využívání některých funkcí MS Excel, který uživatelé dobře znají. Na rozdíl od programů zmíněných výše @RISK pracuje se simulacemi Monte Carlo nebo Latin Hypercube, které získají přesnější rozdělení pravděpodobností vzniku a výskytu rizik. Po provedení simulací program ukáže možné rizikové scénáře a díky předem nastaveným algoritmům budou výstupem doporučené postupy ke snížení rizik a zmírnění jejich dopadu. [12]

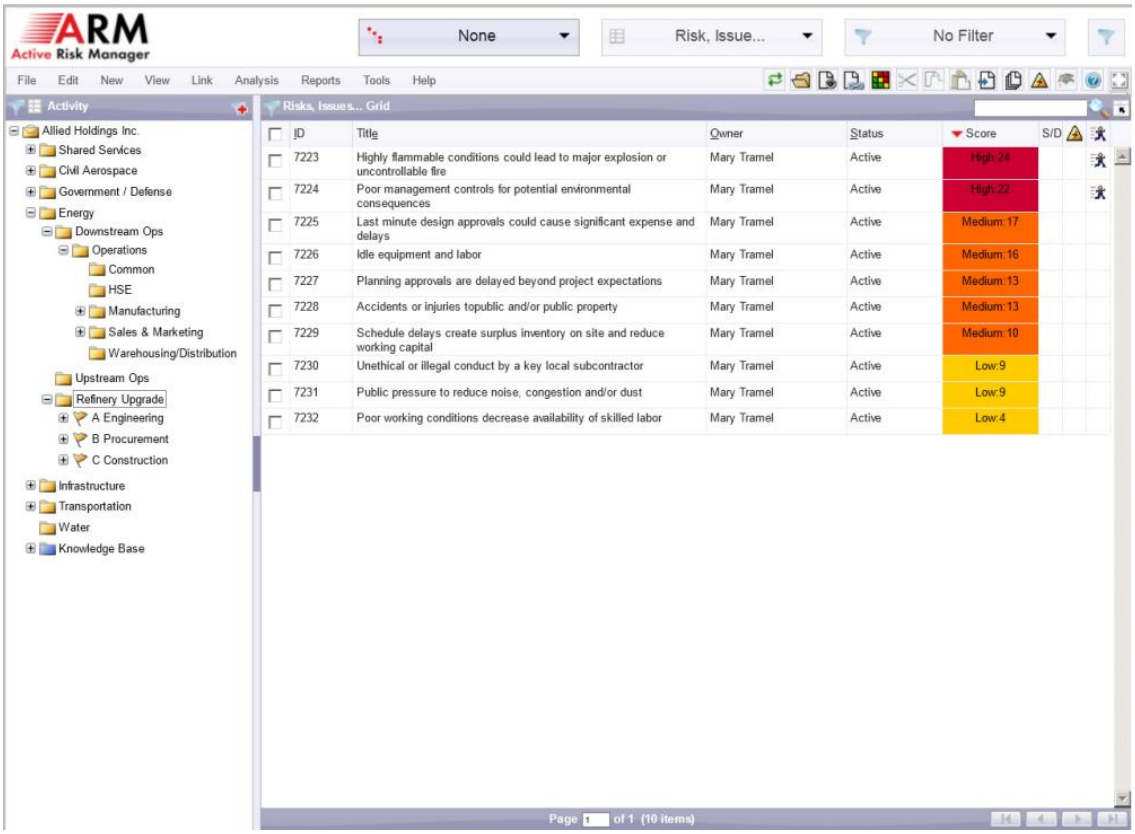
Nevýhodou tohoto programu je jeho složitost, plně využít ho mohou pouze zkušení a školení uživatelé, a při ceně od 1 000 GBP ročně se hodí spíše pro větší podniky a společnosti.



Obrázek 5 – Ukázka výstupů softwaru @RISK[15]

2.2.4. SWORD

Společnost Sword Active Risk dodává softwarové řešení řízení rizik do mnoha průmyslových odvětví. Program pro řízení rizik ARM (Active Risk Manager) lze implementovat v průmyslu, energetice, infrastruktuře, státních organizacích a dalších oblastech. Mimo hlavní produkt ARM společnost dodává 40 specializovaných produktů pro řízení rizik pro odvětvová řešení. Z důvodu vysoké přizpůsobivosti a uživatelské přívětivosti je program vhodný pro většinu středních až velkých podniků a cena se stanoví individuálně dle potřeb zákazníka po konzultaci se zástupcem společnosti Sword.[13]



Obrázek 6 - Ukázka výstupu softwaru ARM[16]

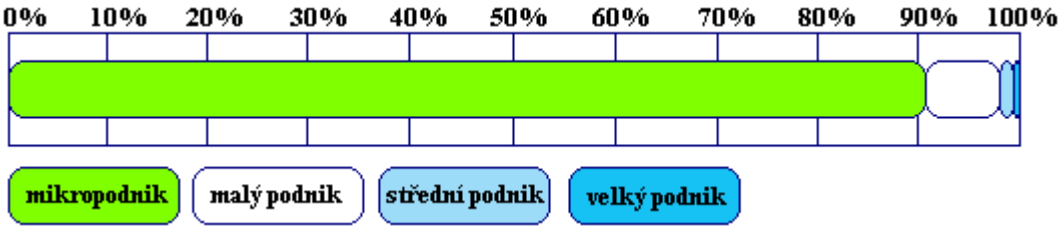
2.3. Hodnocení zvolených SW

	MS Excel	LogicManager	@RISK	SWORD ARM
Cena	V ceně sady MS Office	6 000 - 150 000 USD / ročně	1000 - 1700 GPB / ročně	Cena individuálně podle potřeb zákazníka
Funkce				
Interní audit	-	●	-	●
Simulace	-	-	●	●
Kvalitativní a kvantitativní ohodnocení	-	●	●	●
Mapa rizik (Risk Matrix)	●	●	-	●
Uživatelská přívětivost	1 - Nejlepší, 5 - Nejhorší			
Složitost uživatelského prostředí	1	4	3	4
Náročnost	1	3	3	5
Úroveň potřebných znalostí	1	3	4	5
Technická podpora	5	2	1	1
Celkové hodnocení uživ. Přívětivosti	2	3	3	4
Technické vlastnosti				
Možnost modulového rozšíření	-	●	-	●
Minimální požadavky na konfiguraci PC	Nízké	Střední	Střední	Vysoké
Mobilní / tabletová podpora	●	-	-	●
Webová aplikace	-	-	-	●
Vhodnost pro SME				
Potřeba Rizikového managera	NE	ANO	ANO	ANO
Potřeba administrátora	NE	ANO	ANO	ANO
Potřeba IT oddělení	NE	NE	NE	ANO
Potřeba pravidelných školení	NE	ANO	NE	ANO
Celkové hodnocení vhodnosti pro SME	**2**	**4**	**3**	**5**

Tabulka 1 - Hodnocení SW

Komise Evropského společenství se v roce 2003 usnesla na definici mikropodniků, malých a středních podniků (SME). Střední podnik se definuje jako podnik, který zaměstnává méně než 250 zaměstnanců a jeho roční obrat nepřesahuje 50 milionů EUR nebo jeho bilanční suma roční rozvahy nepřesahuje 43 milionů EUR. Malý podnik, zaměstnává méně než 50 osob a jeho roční obrat nebo bilanční suma roční rozvahy nepřesahuje 10 milionů EUR. Mikropodnik je podnik, který zaměstnává méně než 10 osob a jeho roční obrat nebo bilanční suma roční rozvahy nepřesahuje 2 miliony EUR.[14]

Zastoupení jednotlivých kategorií podniků v EU je uveden na Obr. 7.



Obrázek 7 - Zastoupení kategorií podniků na celkovém počtu v roce 2003 v EU

Konkrétně v České republice podle zprávy Ministerstva průmyslu a obchodu tvořily v roce 2015 malé a střední podniky 99,83 % všech podnikatelských subjektů, tj. 1 139 330 právnických a fyzických osob.[1]

Z důvodu, že podniky SME zastupují největší část všech podniků, se tato práce zaměřuje právě na ně. Pořízení většiny softwarů na dnešním trhu je pro malý či mikropodnik většinou nereálné či neefektivní z důvodů jejich ceny. A ty, které jsou zdarma nebo cenově dostupné nejsou natolik uživatelsky přívětivé, aby se v nich neškolený uživatel dostatečně orientoval a dokázal je správně používat.

Většina neplacených nebo levných programů na řízení rizik funguje na principu jednoduchých tabulek, ve kterých se pracuje se základní rovnicí pro výpočet rizika a to:

$$R = P * I$$

Kde R je míra rizika, P je pravděpodobnost výskytu a I je impakt neboli důsledek rizika. Tato rovnice je efektivní a použitelná pouze v případě vhodného a správného použití jednotlivých proměnných. Často se používá pro dosazení za P a I stupnice od 1 do 10,

kde každé číslo vyjadřuje určitý procentuální rozsah (např. 1 zastupuje 0-10%, 2 zastupuje 11-20% atd.). Klasickým a velkým problémem je možnost stejného výsledku míry rizika pro reálně nesrovnatelná rizika. Lze to ukázat na následujícím příkladu:

Při definování rizik se například uvažuje riziko zemětřesení. Pro použití výše zmíněné rovnice se musí přiřadit hodnoty ze stupnice 1-10 pro pravděpodobnost a pro impakt. Zemětřesení se v České republice v podstatě neobjevuje, a proto je zvolena pravděpodobnost 1% čili 1. Avšak důsledek zemětřesení může být velký a proto impakt se zvolí 90% čili 9. Výsledná míra rizika je tedy 1*9 = 9. Dalším rizikem bude například porucha počítače nebo stroje. Pravděpodobnost je odhadnuta na 25% a důsledek také na 25%. Po převedení se získá 3*3 = 9. Obě rizika mají stejnou míru rizika, čili pro rizikového manažera mají teoreticky stejnou váhu. Ovšem to, že se poškodí stroj nebo počítač je v českých podmínkách reálnější než zemětřesení, tudíž toto riziko by mělo mít větší prioritu.

Dalším problémem je vysoká subjektivnost. V příkladu výše se volily hodnoty pravděpodobnosti a impaktu podle určité stupnice. Každý bod ve stupnici zahrnuje určitý rozsah procent např. 11-20%. Uživatel tak ohodnotil každé riziko a přiřadil určitou hodnotu pro pravděpodobnost a pro impakt podle vlastních zkušeností a znalostí. V případě, že uživatel není v řízení rizik dostatečně školený a zkušený, mohou zde vznikat chybné výsledky na základě nevhodného zvolení hodnot a následná opatření nemusejí vést k očekávanému výsledku celého řízení rizik. Tento proces je možné zobjektivnit použitím vhodných dotazníků a formulářů, které vyplní zaměstnanci podle vlastních zkušeností a znalostí. Následně se zpracují výsledky a vytvoří se nový seznam rizik. Ovšem i zde záleží na subjektivních odpovědích jednotlivých zaměstnanců.

3. Návrh systému řízení

Z předchozí kapitoly vyplývá, že softwary dostupné pro malé podniky, převážně pracující na základním principu kalkulace rizik, tedy pravděpodobnost * impakt, nejsou dostatečně přesné z důvodu velké míry subjektivity, a proto nejsou úplně vhodné pro každého. Klasický přístup k výpočtu míry rizika závisí na zvolených stupnicích pro určení pravděpodobnosti a dopadu. Zde nastává základní problém, a tím je rozsah pro každý bod stupnice. Při volbě škály 1-10 vychází na každý bod rozsah 0-10%. Při volbě například prvního stupně škály, čili 0-10%, ale není zcela jasné, zda se hodnota pohybuje například v rozsahu 0-5% nebo 6-10%. Z hlediska hodnocení rizik to nemusí být vždy dostatečně vypovídající a přesné. Metodika, která by neuvažovala hodnocení rizik tímto stylem, by mohla přinést nový trend v rizikovém managementu. V této kapitole je nastíněno možné řešení tohoto problému.

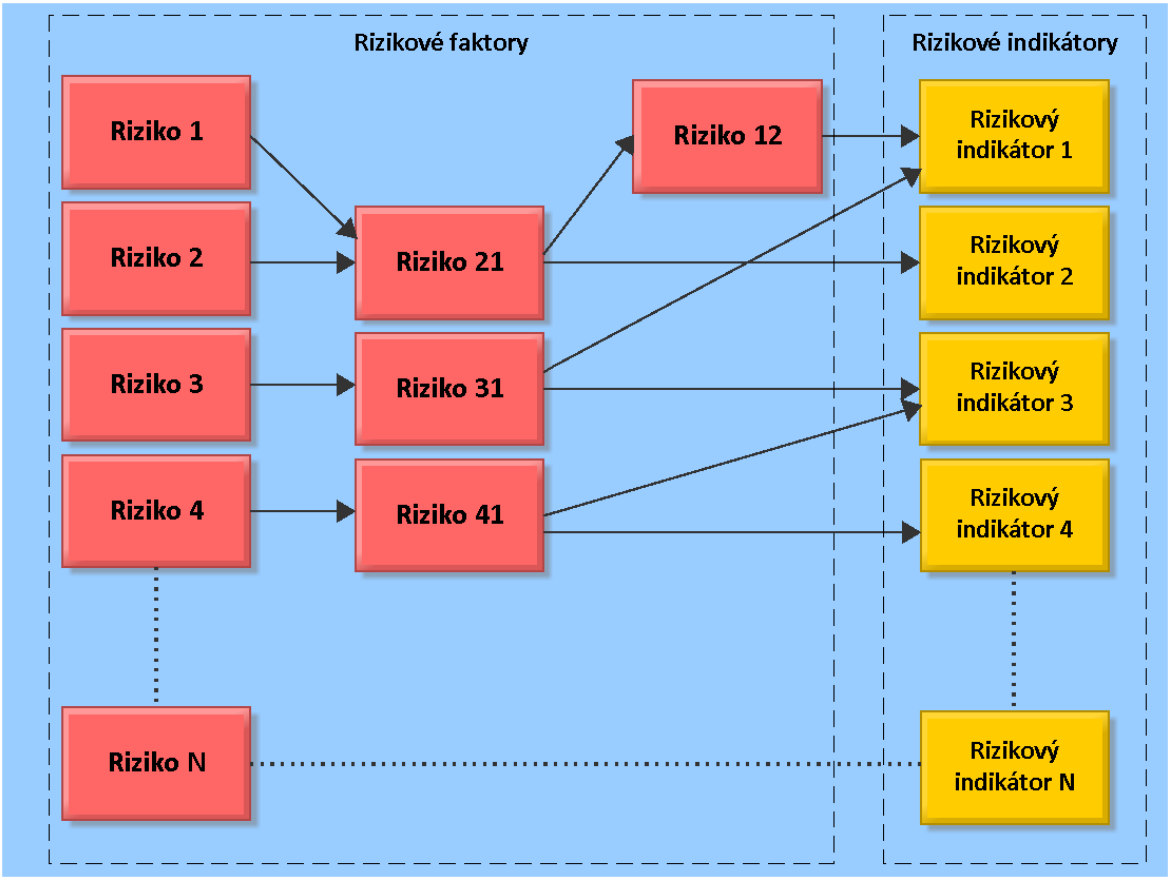
3.1. Nový postup identifikace a hodnocení rizik

Základním postupem identifikace a hodnocení rizik je vypracování seznamu rizik, ve kterém by měla být obsažena většina rizik, které mohou vzniknout pro daný podnik (či projekt). Toho se docílí dotazníky, audity atp. Po zpracování takto získaných dat vznikne seznam rizik, který se v dalším kroku musí ohodnotit z pohledu pravděpodobnosti výskytu a dopadu rizika na podnik. Následně dojde k výpočtu míry rizika podle rovnice R = P*I a z výsledků se určí pořadí jednotlivých rizik podle jejich závažnosti. Tento postup však není dostatečně přesný pro správné zhodnocení rizik a může být i zbytečně rozsáhlý (a tím nepřehledný), protože některá rizika spolu mohou souviset, mohou se podmiňovat nebo ze sebe vyplývat, a s tím základní seznam rizik nepracuje.

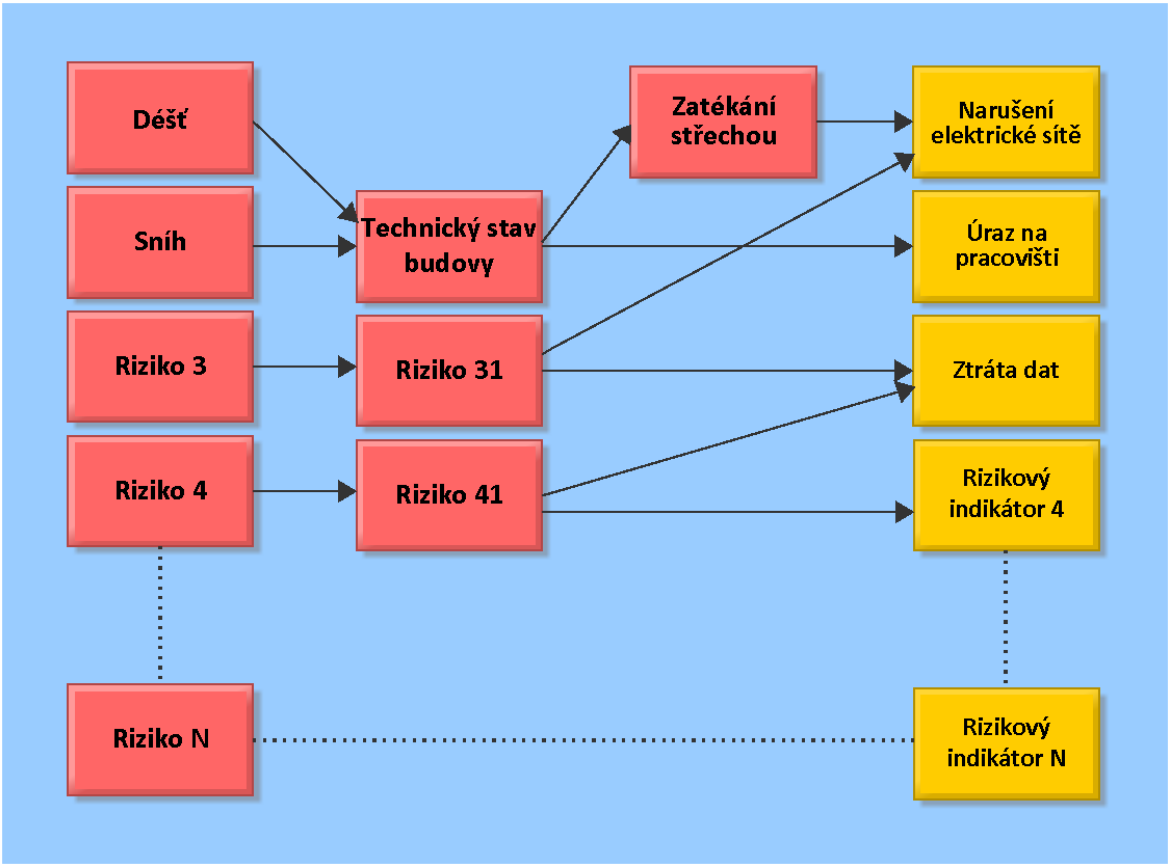
Z toho důvodu se základní seznam rizik nebude hodnotit podle výše zmíněné rovnice, ale bude se upravovat v systému úrovní vysvětleným v následujících kapitolách. Dále se lidé zapojení do řízení rizik rozdělí do skupin podle úrovní jejich zkušeností a znalostí podnikového a rizikového řízení. Každá úroveň bude mít jinou úlohu a uplatnění v celkovém postupu identifikace a hodnocení rizik.

3.2. Úroveň 1

První úroveň by byla základní úrovní v tomto systému. Jejím cílem by bylo vytvoření databáze rizik, se kterou by se dále pracovalo na vyšších úrovních. Podklady potřebné pro vytvoření se získají dotazníky pro zaměstnance a audity v podniku. V této databázi budou vypsaná jednotlivá rizika (rizikové faktory), která vyplynou z podkladů, a která se postupně pospojují podle toho, jak spolu souvisí. Následně se jednotlivé řetězce přiřadí ke klíčovým rizikovým indikátorům, které už lze ohodnotit z pohledu finančního, časového nebo dopadu na kvalitu výrobku. Například budou nalezeny rizika déšť, sníh, technický stav budovy, zatékání střechou, narušení elektrické sítě atp. Všechny spolu nějak souvisí a dohromady tvoří řetězce, kde na konci je rizikový indikátor (např. ztráta dat, úraz na pracovišti…). Ukázka výstupu Úrovně 1 je na Obrázku 8 a Obrázku 9 níže.



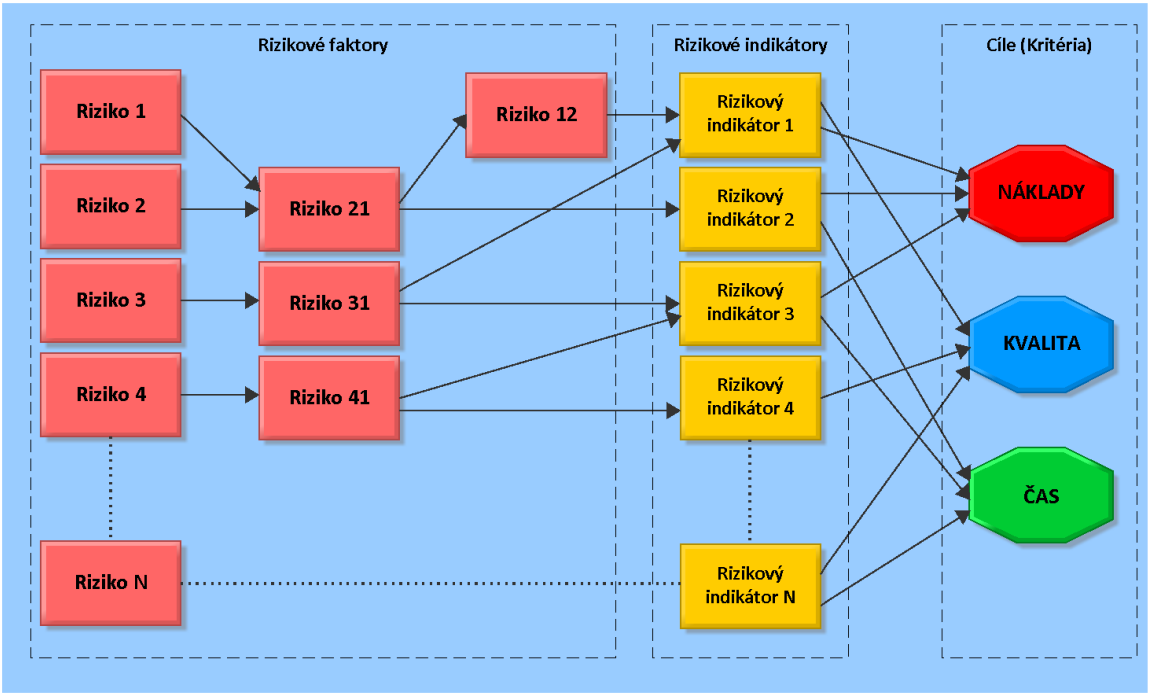
Obrázek 8 - Obecný grafický výstup úrovně 1



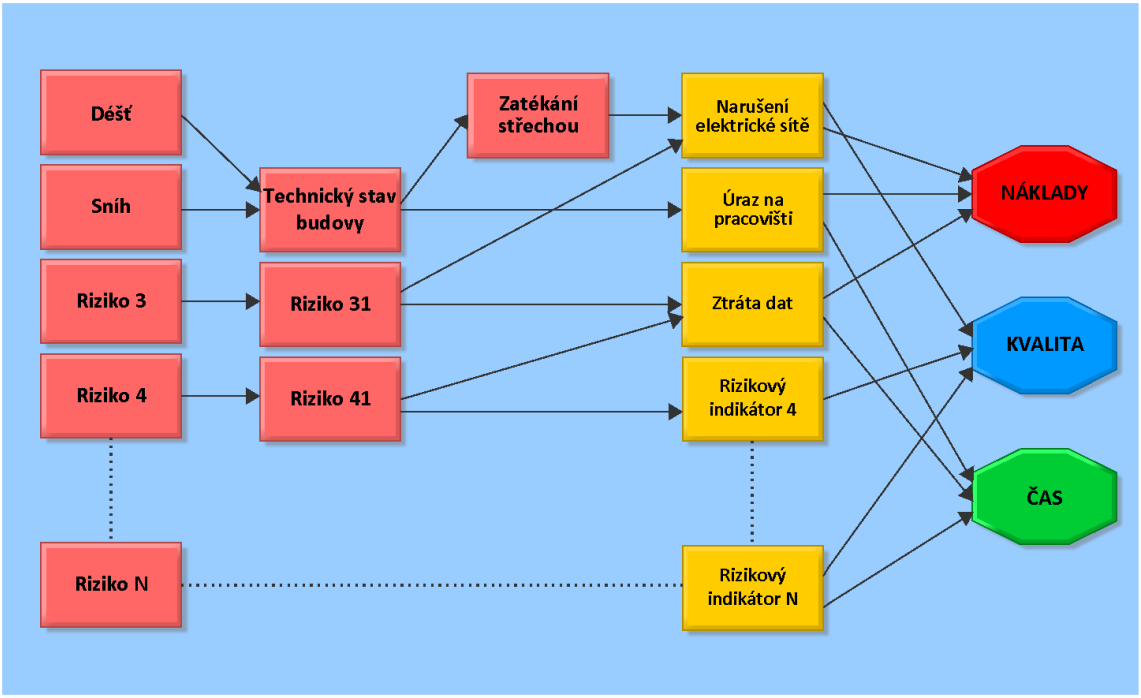
Obrázek 9 – Grafický výstup úrovně 1 (konkrétní případ rizikových scénářů)

3.3. Úroveň 2

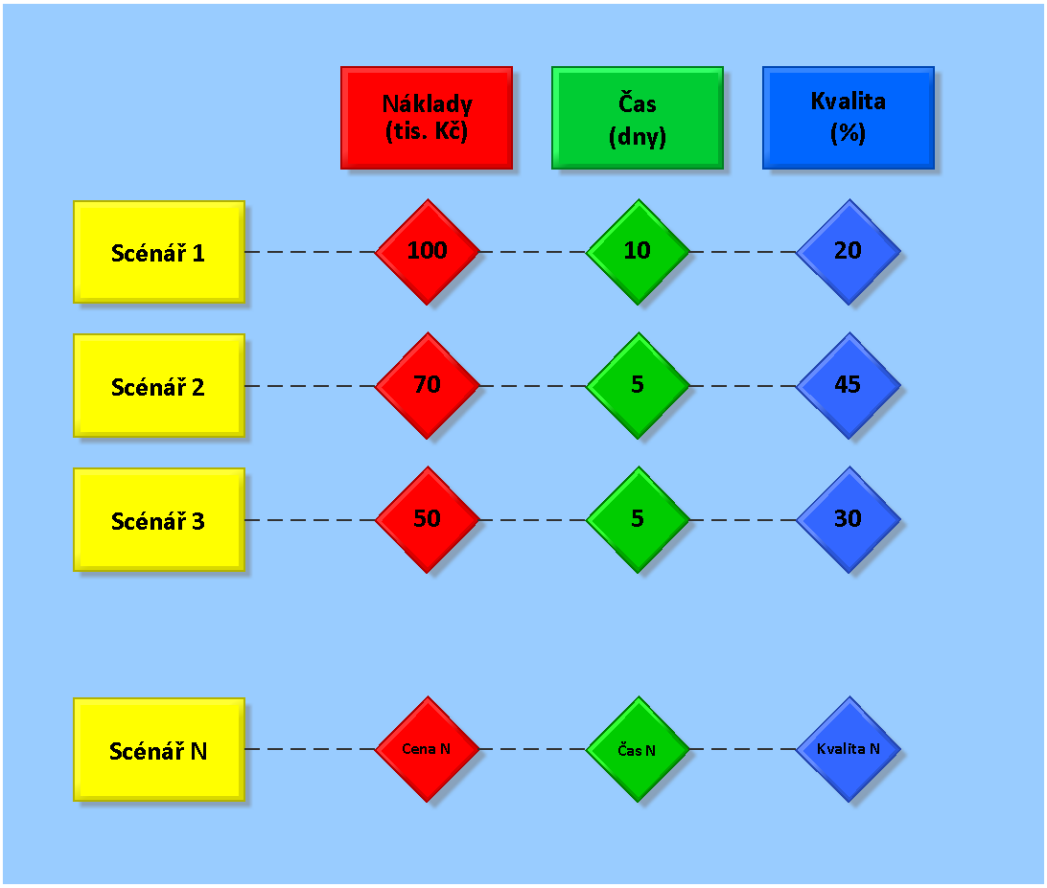
Ve druhé úrovni dojde k hodnocení jednotlivých rizikových indikátorů podle toho, zda mají dopad na kvalitu, náklady nebo čas potřebný k vytvoření konečného produktu. To jsou tři hlavní kritéria, která ovlivňují chod a případný zisk firmy. Po pospojování jednotlivých rizikových faktorů a indikátorů s těmito kritérii vzniknou rizikové scénáře, které mohou nastat s jasně určeným dopadem na podnik. Dalším krokem bude kvantifikace dopadu výskytu jednotlivých rizik. Tedy jaký bude mít daný scénář finanční, časový dopad nebo jaký bude mít dopad na kvalitu produktu. Po dokončení odhadů se všechny scénáře srovnají podle jejich závažnosti, aby se později co nejpřesněji určilo, co je z pohledu rizikového managementu více či méně důležité. Tyto odhady jsou klíčové pro následné návrhy protiopatření, tudíž je potřeba, aby pracovníci, zabývající se touto částí procesu, byli dostatečně zkušení v chodu podniku a problematice řízení rizik. Tím budou schopni správně odhadnout dopady jednotlivých rizikových scénářů na výše zmíněná kritéria. Takto vzniklá data se mohou použít v simulacích, které je zpřesní a následně se mohou na jejich základě zpětně upravit data získaná v předchozích krocích. Touto částí procesu získáme vhodnější a přesnější výsledky, než při použití rovnice na ohodnocení rizik R = P * I. Tyto výsledky pomohou s rozhodováním, zda je riziko přijatelné, nebo jestli je potřeba zavést protiopatření. Na Obrázku 10 – 12 níže jsou zobrazeny výstupy úrovně 2 po prvním a druhém kroku.



Obrázek 10 - Obecný grafický výstup druhé úrovně po prvním kroku



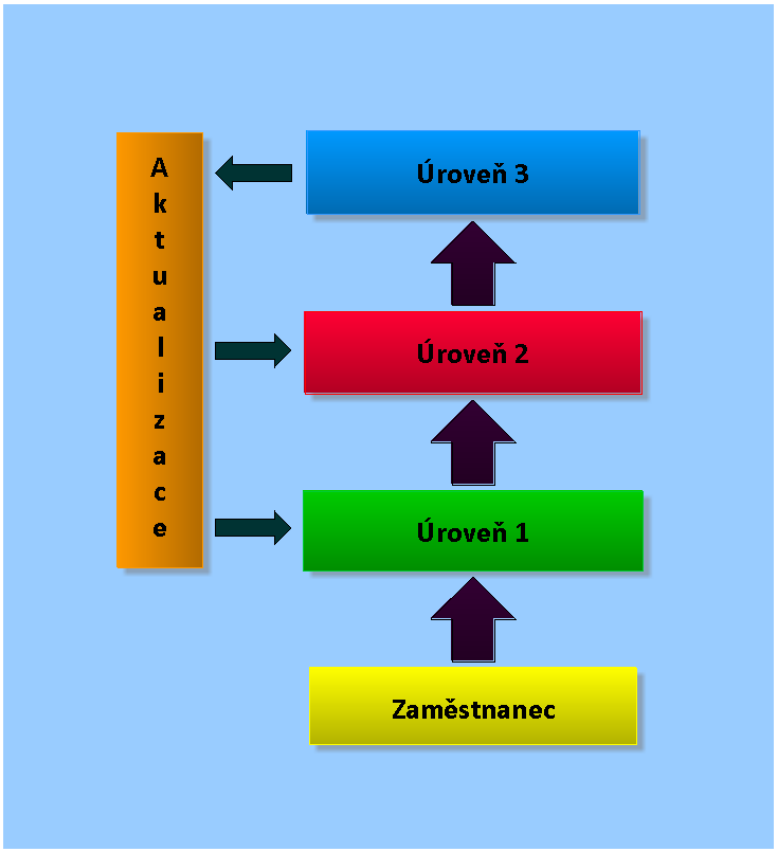
Obrázek 11 - Grafický výstup úrovně 2 po prvním kroku (přiřazení rizikových indikátorů na hlavní kritéria)



Obrázek 12 - Výstup úrovně 2 po druhém kroku (kvantifikovaný odhad rizikových scénářů)

3.4. Úroveň 3

Lidé pracující s třetí úrovní budou mít za úkol na základě výsledků z Úrovně 2 vytvořit a následně uplatnit protiopatření na zmírnění následků jednotlivých rizikových scénářů či jim úplně předejít. Dále budou podle dosažených výsledků zpětně aktualizovat databázi v předchozích úrovních. Tato zpětná vazba umožní jistou predikci pro budoucí scénáře. Když nastane podobný případ, který se již jednou řešil, tak tento systém ukáže, jaká opatření se aplikovala a jakých výsledků se tím dosáhlo. To do budoucna urychlí proces řízení rizik.



Obrázek 13 - Úroveň 3

3.5. Shrnutí nového systému řízení

Přiřazením pracovníků do tří úrovní na základě jejich zkušeností a znalostí risk managementu a podniku se docílí efektivního rozdělení celého procesu řízení rizik. Každá z těchto úrovní provede určitou část postupu a během celého procesu se mohou zpětnou vazbou navzájem doplňovat a upravovat podle dosažených výsledků. Celý postup procesu je znázorněn na Obrázku 14 v Příloze A v kapitole Přílohy. Touto zpětnou vazbou se dosáhne přesnějších výsledků a celkově to zefektivní celý proces.

Touto modifikací se dospělo k jednoduchému a přesnému nástroji na řízení rizik, který se tím hodí i pro mikro a malé podniky. Může nahradit drahé a náročné programy, které jsou dnes běžně k dispozici a tím zpřístupní risk management i pro SME, které ho velmi často vůbec neřeší.

Na Obrázku 14 v Příloze A jsou znázorněny jednotlivé kroky pro každou úroveň. Softwarové zpracování tohoto modifikovaného procesu, který tímto systémem vznikne, by tedy mělo vycházet z tohoto návrhu. Tyto úpravy jsou inspirovány výstupními materiály projektu RiMaCon, který se zabýval vývojem softwaru pro řízení rizik v rámci SME. Tohoto projektu se účastnila i Západočeská Univerzita.

Závěr

Cílem této práce bylo teoreticky popsat metodiku řízení rizik, provést rešerši na poli softwarů určených pro řízení rizik a z nich vybrat a popsat některé zástupce. Dále navrhnout jednoduchou metodiku pro systém řízení rizik s cílem zlepšení stávajícího systému, který bude aplikovatelný při vývoji softwaru pro risk management, speciálně určený pro malé a střední podniky.

V první kapitole je definován pojem riziko. Z rešerše vyplývá, že riziko se popisuje různě, podle oblasti jeho vzniku. Obecně ale znamená jistou pravděpodobnost vzniku neočekávané události, která může mít negativní dopad na očekávaný výsledek. Riziko je zjednodušeně určeno pravděpodobností vzniku a jeho závažností. Z toho vychází základní rovnice pro určení míry rizika R = P*I. Tato rovnice se používá jako nejjednodušší nástroj pro určení rizika. Používá se i v programu MS Excel a dalších jednoduchých programech pro řízení rizik. Dále se zde ukazují jednotlivé metody a typy analýz, které se v procesu řízení rizik používají. Na základě první kapitoly se domnívám, že důkladně provedená analýza rizik je klíčová pro úspěšné zvládnutí celého procesu řízení rizik.

Důkladnou analýzou se jasně definují rizika. Určí se jejich dopad na chod podniku a možné vzniklé ztráty. Tím se zjistí, která rizika jsou akutní, a která nejsou tolik důležitá a mohou se řešit později. Následně se volí vhodná protiopatření v závislosti na jejich ekonomických nákladech a přínosech. Díky dobře zvládnutému managementu rizik se dosáhne vyššího profitu a lepší plynulosti chodu podniku.

V rámci druhé kapitoly byli vybráni čtyři zástupci z velkého výběru programů na trhu pro řízení rizik. Mezi nimi jsou zástupci jednoduchých a dostupných softwarů, ale i velkých a složitých programových balíků. V rámci porovnání byl každý software zkoumán z hlediska jeho ceny a dostupnosti, složitosti a uživatelské přívětivosti a jeho dostupných funkcí. Jako zástupce jednoduchých programů byl zvolen MS Excel, který lze použít jako jednoduchý matematický procesor, který určí hodnoty míry rizika a je schopný vytvořit jednoduché grafické výstupy v podobě grafů a tabulek. Další zástupce je LogicManager, který poskytuje zdarma předlohu pro MS Excel. Tato předloha umožňuje vyplněním přednastavených formulářů generovat grafické výstupy v podobě mapy rizik. Kromě toho LogicManager poskytuje profesionální software, který usnadňuje řízení rizik ve všech odvětvích a činnostech podniku. Nevýhodou

je jeho vyšší náročnost a složitost, stejně jako jeho vysoká cena. @RISK a SWORD ARM jsou rozsáhlé a složité programové celky, které jsou schopny pokrýt různé oblasti podnikání a zajistit komplexní řízení rizik v celé společnosti. @RISK je navíc schopen provádět simulace Monte Carlo nebo Latin Hypercube, které zpřesňují výsledky hodnocení rizik. Z důvodu jejich vysoké ceny a rozsáhlosti jsou vhodné pro větší společnosti, které mají dostatečně zkušené rizikové manažery nebo týmy, které se zabývají řízením rizik podniku. Pro řízení rizik v rámci SME je dle mého názoru nejvíce použitelný MS Excel z důvodu jeho cenové dostupnosti a jednoduchosti. Ovšem jeho nevýhodou je nepřehlednost tabulek v případě rozsáhlejších rizikových databází a také náchylnost k chybám v důsledku nevhodně zvolených proměnných v rovnici R = P*I, se kterou se zde pracuje.

V poslední kapitole je navrhnuta funkcionalita softwaru pro řízení rizik v rámci SME. S ohledem na rešerši z první části a z části porovnání softwarů byl zvolen odlišný přístup pro hodnocení rizika. V tomto postupu se rozdělí pracovníci do jednotlivých úrovní, podle jejich zaměření a zkušeností s řízením rizik. Každá úroveň zpracovává určitou část v celkovém procesu řízení rizik. Cílem tohoto rozdělení je zpřesnění vstupních hodnot analýzy vedoucí k přehlednějším a přesnějším výsledkům. V první úrovni je hlavním úkolem tvorba seznamu jednotlivých rizikových faktorů, s možností tvorby hierarchické struktury a to hlavně z důvodu vzájemné interakce rizikových faktorů a lepšího pochopení rizikových scénářů. Ve druhé úrovni jsou tvořeny rizikové scénáře. Scénáře jsou poté kvantitativně analyzovány z pohledu nákladů, kvality a času. Z toho vyplývá, že lidé, podílející se na druhé úrovni, musí mít nezbytné znalosti o chodu podniku, aby dokázali správně určit míru dopadu jednotlivých scénářů. Tím vznikne jasný a přehledný seznam, ze kterého může třetí úroveň navrhnout a aplikovat protiopatření vedoucí k minimalizaci jednotlivých rizik a jejich dopadu. Následně může zpětnou vazbou upravovat a aktualizovat seznamy v předchozích úrovních podle efektu následně použitých opatření. Hlavním přínosem této jednoduché modifikace základních postupů řízení rizik je usnadnění a zjednodušení hlavní části řízení rizik, a to analýzy rizik. Díky tomuto postupu budou mít rizikoví manažeři snadnější práci, která povede k lepším výsledkům pro zlepšení chodu podniku. Toto řešení je vhodné i pro střední, malé a mikro podniky. Metodiku jsem navrhoval a částečně modifikoval dle výstupních materiálů projektu RiMaCon, do kterého se zapojila i Západočeská Univerzita. Tento projekt se zabýval vývojem softwaru pro řízení rizik v rámci SME. Cílem této práce bylo mimo jiné také

přispět rešeršní činností a vlastním zhodnocením navrhované metodiky v rámci zmíněného projektu. Návrhy na zlepšení metodiky a výstupy této práce byly v rámci konzultací prezentovány členům projektu.

Seznam použité literatury

[1] "Ministerstvo průmyslu a obchodu." [Online]. Dostupné z: https://www.mpo.cz//cz/podnikani/male-a-stredni-podnikani/studie-a-strategicke-dokumenty/zprava-o-vyvoji-maleho-a-stredniho-podnikani-a-jeho-podpore-v-roce-2015--221710/.

[2] V. Smejkal and K. Rais, *Řízení rizik ve firmách a jiných organizacích*, 3. Praha: Grada Publishing, 2010.

[3] V. Smejkal and K. Rais, *Řízení rizik ve firmách a jiných organizecích*, 4. Praha: Grada Publishing, 2013.

[4] VeberJaromír, *Management*, 2nd ed. Praha: Management press, 2009.

[5] M. Korecký and V. Trkovský, *Management rizik projektů se zaměřením na projekty v průmyslových podnicích*, 1. Praha: Grada Publishing, 2011.

[6] J. Kruliš, *Jak vítězit nad riziky*. Praha: Linde Praha, 2011.

[7] "Úřad pro technickou normalizaci, metrologii a státní zkušebnictví." [Online]. Dostupné z: http://www.unmz.cz/test/management-rizik-r913.

[8] "International Organization for Standardization." [Online]. Dostupné z: http://www.iso.org/iso/home/standards/iso31000.htm.

[9] "Management Mania." [Online]. Dostupné z: www.managementmania.com.

[10] "Bright Hub Project Management." [Online]. Dostupné z: http://www.brighthubpm.com/risk-management/88381-using-excel-to-make-a-risk-assessment-template/.

[11] "LogicManager." [Online]. Dostupné z: http://www.logicmanager.com/erm-software/product/.

[12] "Risk - Jihočeská Univerzita." [Online]. Dostupné z: http://risk.ef.jcu.cz/index.php.

[13] "Datacons." [Online]. Dostupné z: http://www.datacons.cz/index.php/produktove-reseni/interni-audit.

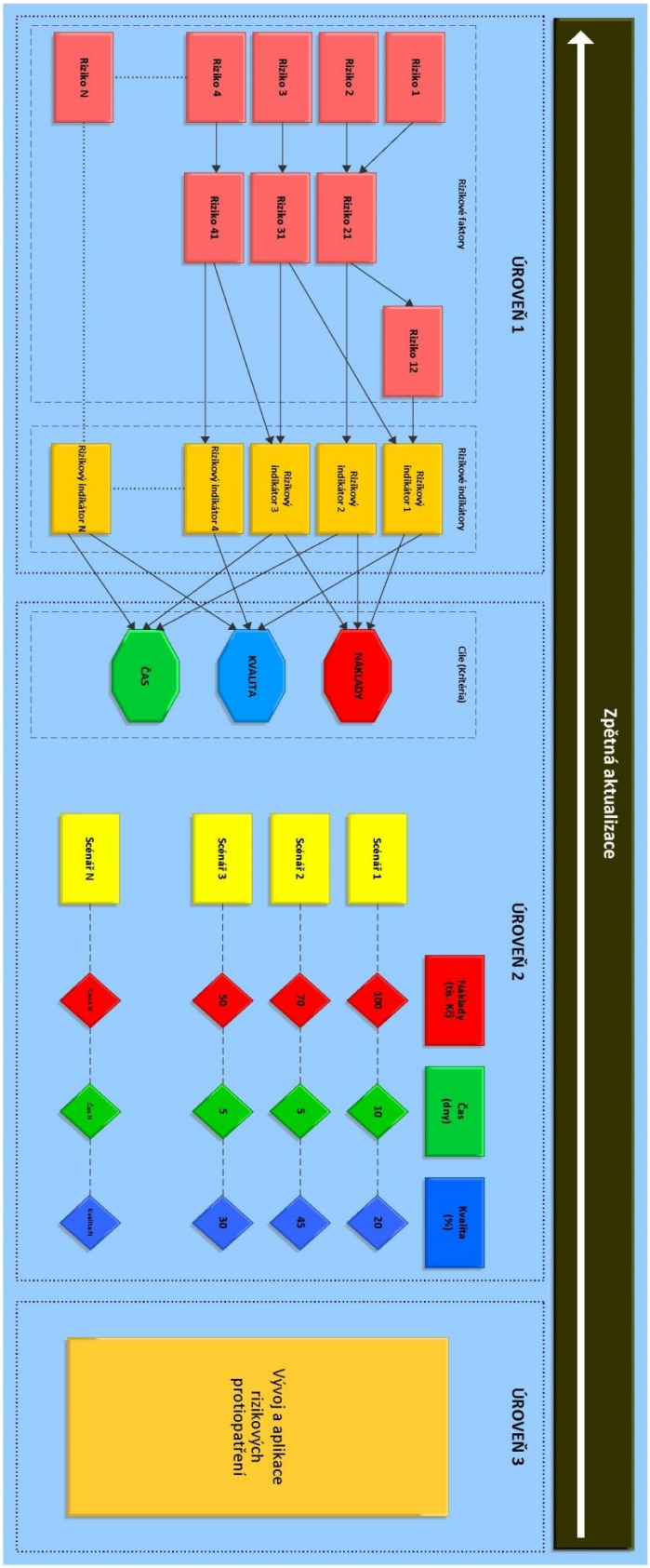
[14] "Unie malých a středních podniků ČR." [Online]. Dostupné z: http://www.sme-union.cz/definice-sme/.

[15] "Palisade - @RISK." [Online]. Dostupné z: http://www.palisade.com/risk/.

[16] "SWORD ARM." [Online]. Dostupné z: http://www.sword-activerisk.com/products/active-risk-manager-arm/.

Přílohy

Příloha A - Shrnutí procesu řízení rizik



Obrázek 14 - Shrnutí nového procesu řízení rizik