Metody analýzy rizik v oblasti ochrany majetku

Bc. Tomáš Zelina

Diplomová práce
2014

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2013/2014

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Tomáš Zelina**
Osobní číslo:	**A11706**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**prezenční**
Téma práce:	**Použití metod analýzy rizik v oblasti ochrany majetku**
Téma anglicky:	**The Use of Risk Analysis Methods in the Asset Protection Field**

Zásady pro vypracování:

1. **Pojednejte o bezpečnostním managementu a požadavcích na řízení rizik.**
2. **Analyzujte bezpečnostní aspekty ochrany majetku.**
3. **Rozeberte podstatu a princip metod analýzy rizik.**
4. **Posuďte vhodnost jednotlivých metod analýzy rizik pro oblast ochrany majetku.**
5. **Navrhněte možnosti využití metod analýzy rizik při ochraně majetku.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **LUKÁŠ, Luděk, a kol. Bezpečnostní technologie, systémy a management II. Zlín: VeRBum, 2012. 384 s. ISBN 978-80-87500-19-4.**
2. **LUKÁŠ, Luděk, a kol. Bezpečnostní technologie, systémy a management III. Zlín: VeRBum, 2013. 456 s. ISBN 978-80-87500-035-4.**
3. **ŠAJDLEROVÁ, Ivana; KONEČNÝ, Milan. Základy managementu. Ostrava: Ediční středisko VŠB TUO, 2007. 197 s. ISBN 978-80-248-1520-6.**
4. **HURTA, Josef; LAUCKÝ, Vladimír. Management bezpečnostního inženýrství. Zlín: Univerzita Tomáše Bati ve Zlíně, 2005. 172 s. ISBN 80-7318-412-5.**
5. **LAUCKÝ, Vladimír. Technologie komerční bezpečnosti I. Zlín: Univerzita Tomáš Bati ve Zlíně, 2009. 82 s. ISBN 978-80-7318-889-4.**
6. **ZEMAN, Petr. Česká bezpečnostní terminologie: výklad základní pojmů. Brno: Masarykova univerzita v Brně, 2003. 186 s. ISBN 80-210-3037-2.**
7. **ŠEFČÍK, Vladimír. Analýza rizik. Zlín: Univerzita Tomáše Bati ve Zlíně, 2009. 98 s. ISBN 978-80-7318-696-8**
8. **ČSN EN 31010. Management rizik: Techniky posuzování rizik. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011. 80 s.**

Vedoucí diplomové práce: **doc. Ing. Luděk Lukáš, CSc.**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **7. února 2014**

Termín odevzdání diplomové práce: **27. května 2014**

Ve Zlíně dne 7. února 2014

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- Že odevzdaná verze diplomové/bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

ABSTRAKT

Předmětem diplomové práce je shrnutí problematiky bezpečnostního managementu, řízení rizik a dále analyzovat bezpečnostní aspekty ochrany majetku. V další části práce je kladen důraz na jednotlivé metody analýz rizik a jejich využití právě pro oblast ochrany majetku. V závěru práce jsou vybrané metody analýz rizik aplikovány pro vybrané oblasti ochrany majetku.

Klíčová slova:

Bezpečnost, hrozba, riziko, analýza rizik, řízení rizik, majetek, aktivum, bezpečnostní opatření

ABSTRACT

The subject of the thesis is a summary of the issues of safety management, risk management and analyze safety aspects of the property. In the next section the emphasis is on individual risk analysis methods and their usage for Aseet Protection. In conclusion, there are some areas of risk analysis applied to certain areas of asset protection.

Keywords:

Safety, threat, risk, risk analysis, risk management, property, asset, security measures

Poděkování:

Chtěl bych poděkovat vedoucímu diplomové práce panu doc. Ing. Luďkovi Lukášovi, CSc. za odborné vedení, cenné rady a připomínky, které mi poskytoval během práce.

Dále bych chtěl poděkovat rodinně, která mě po celou dobu studia podporovala.

OBSAH

ÚVOD

V dnešní době, kdy jsou ve světě velké majetkové rozdíly, jsou lidé stále více nuceni k tomu, aby si svůj majetek chránili. S rozvojem informačních technologií se nejedná pouze o majetky fyzické nebo finanční podstaty, ale jedná se také o bezpečnost a ochranu informací.

Možnost, jak si chránit svůj majetek, je velké množství, ale vybrat tu nejlepší a nejefektivnější možnost s vynaložením co možná nejmenších nákladů, představuje mnohdy nelehký úkol.

V úvodu své práce jsou uvedeny jednotlivé funkce managementu, jejich popis, vzájemná návaznost a propojenost. Jedná se o funkce, jejichž znalost je pro činnost manažerů na všech úrovních managementu nezbytná.

V další části práce jsou vymezeny termíny z oblasti řízení rizik a základní vztahy mezi nimi. Proces řízení rizik se skládá z dílčích subprocesů, z nichž je v práci kladen důraz na subproces posuzování rizik.

Stěžejní kapitoly práce jsou věnovány metodám analýz rizik. Analýza rizik představuje velmi důležitou část v procesu řízení rizik, konkrétně v subprocesu posuzování rizik. Metody analýz rizik zasahují do oblastí bezpečnostního managementu, průmyslu komerční bezpečnosti, návrhů bezpečnostních systémů, krizové infrastruktury a do mnoha dalších odvětví sloužící k ochraně života, zdraví, přírody a majetku.

Jednotlivé metody analýz rizik jsou důkladně popsány a následně některé z nich využity v oblasti ochrany majetku.

I. TEORETICKÁ ČÁST

1 MANAGEMENT

Většina odborné veřejnosti by vznik pojmu management zařadila nejspíš do druhé poloviny 20. století. Ovšem management je mnohem starší. Jeho počátky sahají daleko do historie, kdy bylo například nutné řídit armády, řídit přepravu potravin a jiné.

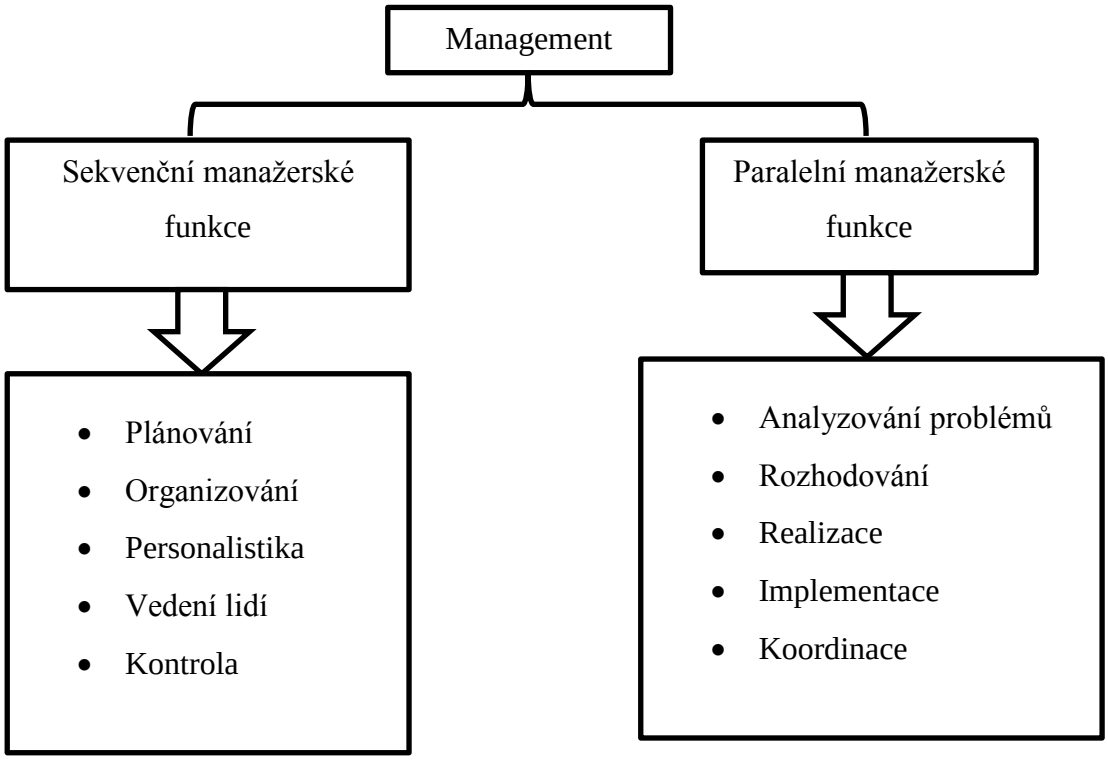
Ovšem management jako obor se začal formovat již na konci 19. století. Prošel řadou vývojových období a vždy se na něj pohlíželo jinak. A proto také definice, resp. popis managementu není úplně jednoznačný, ale často se liší. Příkladem rozdílu jsou následují definice:

Management je proces tvorby a udržování prostředí, ve kterém jednotlivci pracují společně ve skupinách a účinně dosahují vybraných cílů (Koontz, H., Weihrich, H.)

Management je vykonávání věcí prostřednictvím ostatních lidí. Je umění dosahovat cíle organizace rukama a hlavami jiných (Pale E.)

Management je proces plánování, organizování, personálního zajištění, vedení a kontroly organizačních činností zaměřených na dosažení cílů podniku. (Chung K. H.)

Z analýz uvedených definic managementu plyne, že základem managementu je vytyčení cílů, vytvoření plánů a následné splnění jejich cílů za pomocí lidí.



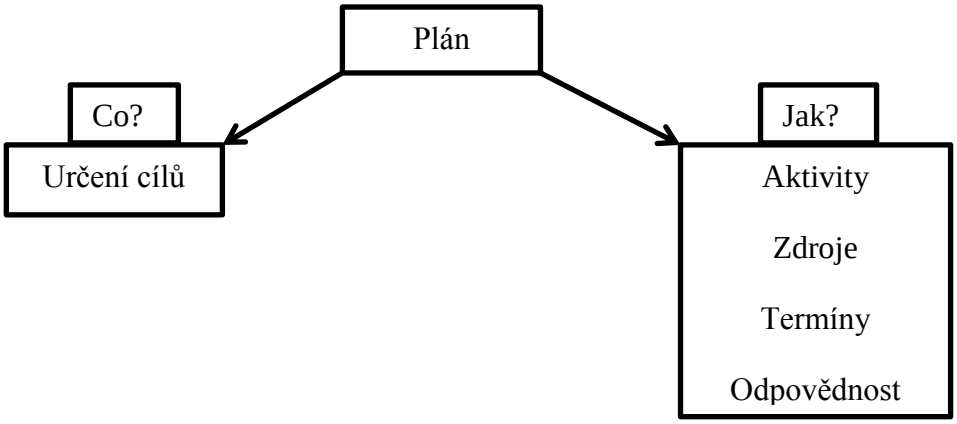
Obr. 1 Rozdělení a funkce managementu, vlastní zdroj

1.1 Sekvenční funkce managementu

Sekvenční funkce se realizují postupně a prostupují jimi funkce paralelní.

1.1.1 Plánování

Plánování je prvotní manažerskou funkcí, jejímž úkolem je stanovit cíle a způsoby, jak těchto cílů dosáhnout ve stanoveném čase. Výsledkem procesu plánovaní je plán.



Obr. 2 Plán, vlastní zdroj

Cíl v rámci procesu plánování představuje konkrétní budoucí výsledek, dílo, stav, kterého má být dosaženo. Při stanovení cíle se vychází z následujících požadavků:

- dodržení priorit,
- měřitelnost výsledků,
- přiměřenost vzhledem ke zdrojům a k okolí.

Aktivity představují činnosti, procesy a opatření, jejichž plněním se dosahuje požadovaných cílů.

Zdroje mohou být materiální i nemateriální povahy a jsou nezbytné k splnění plánu. Zdroje představují:

- finanční prostředky,
- pracovníci s požadovanou kvalifikací,
- materiální zabezpečení,
- informační a technologické zabezpečení,
- know-how.

Termín znamená poslední den, nebo lhůtu pro splnění daného úkolu. Podle složitosti úkolu může být termín rozdělen na několik dílčích termínů.

Odpovědností se rozumí stanovení konkrétní osoby, která zodpovídá za splnění dílčího nebo celkového úkolu.[3]

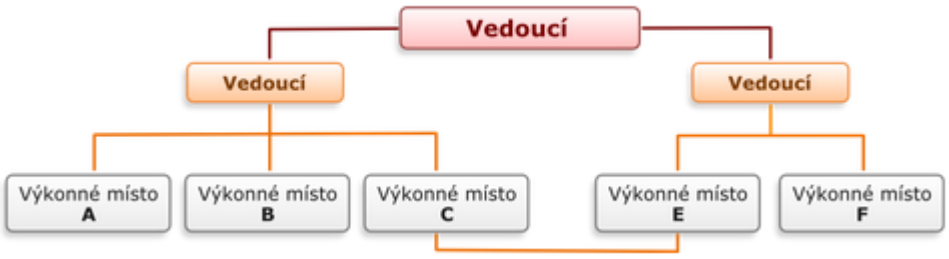
1.1.2 Organizování

Organizování je cílevědomá činnost, která si klade za cíl uspořádat prvky v systému, jejich aktivity, koordinaci a kontrolu tak aby přispěly maximální měrou k dosažení stanovených cílů. Výsledkem organizování je organizační struktura.

Organizační struktura je systém, který umožňuje efektivní provádění činností. Je tvořena složkami a vztahy mezi nimi. Těmito vztahy mezi složkami jsou nadřízenost, podřízenost a rovnocennost. Každá organizační skupina by měla být vytvořena tak, aby bylo zřetelné, kdo a jaké úkoly má plnit a kdo je zodpovědný za výsledky.

Modely organizačních struktur:

- liniový typ,
- liniově štábní typ,
- funkční typ,
- maticový typ.[3]



Obr. 3 Ukázka organizační struktury liniového typu [12]

Z výše zmíněného vyplývá, zdali máme stanovený plán, je nutné vytvořit organizační strukturu, která bude dohlížet na plnění cíle, nebo dílčích cílů plánu. Je nutné zvolit vhodnou koncepci organizační struktury, aby nedošlo k nesrovnalostem při plnění cílů plánu.

1.1.3 Personalistika

Personalistika se zaměřuje na získávání a dosazování jednotlivců či skupin lidí, kteří pracují na přidělených místech a přispívají k dosažení cílů organizace. Personalistika znamená obsazování pozic v organizační struktuře a udržování jejich obsazení.

Cílem personalistiky je tedy zabezpečit dostatečný počet kvalifikovaných lidí, kteří budou vhodní pro naplnění cílů organizace. Vhodnost, jednotlivých uchazečů je realizována zejména na základě:

- pohovorů:
  - individuální pohovory,
  - pohovorové panely,
  - výběrová komise.
- assessment centrum [3]

Další náplní personalistiky je vzdělávání zaměstnanců pomocí kurzů, odborných přednášek nebo školení.

1.1.4 Vedení lidí

Znamená ovlivňování jednotlivců, skupin lidí, takovým způsobem, který zabezpečí plnění cílů organizace. Náplní této funkce je zejména schopnost:

- vést,
- motivovat,
- ovlivňovat,
- usměrňovat.

Obr. 4 Vedení lidí [12]

1.1.5 Kontrolování

Kontrolování představuje zpětnou vazbu, pomocí které manažeři získávají objektivní představu o splnění či nesplnění dříve zadaných úkolů. Cílem kontroly je dosáhnout jistoty, že prvotní plány jsou úspěšně realizovány. V případě zjištění odchylek v plánu je potřeba vytvořit a přijmout nápravná opatření.

Význam kontroly spočívá zejména v těchto činnostech:

- Zaměření úsilí správným směrem – procesy kontrol pomáhají zjistit, zda všechny naplánované činnosti byly vykonány správně.
- Monitorování a hodnocení činností – díky kontrole manažeři monitorují a hodnotí, zdali bylo dosaženo takové chování a činnosti, jaké si organizace přeje.
- Koordinování činností – kdyby nebylo kontroly, zaměstnanci i manažeři by mohli jednat mnoha různými způsoby.
- Snižování nejistoty – při opakujících se situacích kontrola snižuje nejistotu manažerů při rozhodování, neboť kontrola určuje jak takové situace řešit.

Typy kontrolních procesů:

- Vnější kontrola
- Vnitřní kontrola
    - běžná vnitřní kontrola,
    - kontrola prováděná podnikovým útvarem,
    - interní audit,
    - preventivní kontrola,
    - průběžná kontrola,
    - kontrola zpětnou vazbou.[3]

Obr. 5 Typy kontrolních procesů [12]

1.2 Paralelní funkce managementu

Jedná se o funkce průběžné, které jsou uskutečňovány při většině sekvenčních manažerských funkcí.

1.2.1 Analyzování problémů

Analyzování problémů je prvotním předpokladem, aby se mohlo problému zabránit nebo alespoň minimalizovat možnost jeho vzniku. Analýza znamená hledání, určení a pochopení podstaty a vzniku problému.

1.2.2 Rozhodování

O rozhodování se mluví tehdy, je-li k dispozici možnost volby nejméně ze dvou možných řešení na základě určených kritérií. Rozhodování je jádrem řízení a uplatňuje se ve všech manažerských činnostech. Kvalita a výsledky rozhodovacích procesů ovlivňují zásadním způsobem efektivnost fungování a budoucí prosperitu celé organizace.

Rozhodovací proces může být za následujících podmínek:

- za jistoty,
- za rizika,
- za nejistoty.

Podle závažnosti rozhodovacích procesů dělíme rozhodnutí na:

- strategická,
- taktická,
- operativní.

Pro manažera existují dva základní typy rozhodovacích problémů:

- Dobře strukturované problémy:
    - jednoduché,
    - opakované,
    - programované.
- Špatně strukturované problémy:
    - nové a neopakovatelné,
    - větší množství faktorů ovlivňující řešení,
    - nejistota budoucího vývoje faktoru. [3]

1.2.3 Realizace

Realizace je uskutečnění cílů organizace pro co nejlepší dosažení cílů organizace. Jedná se zejména o zavedení nových systémů, nové organizační uspořádání či využívání zcela nových progresivních trendů. Patří zde také vylepšení zařízení, inovace systému a softwaru.

1.2.4 Koordinace

Zajišťuje soulad mezi jednotlivými cíli organizace, jeho složkami a činnostmi. Je realizována ve všech funkcích řízení. Koordinace je prováděna nejčastěji pomocí porad.

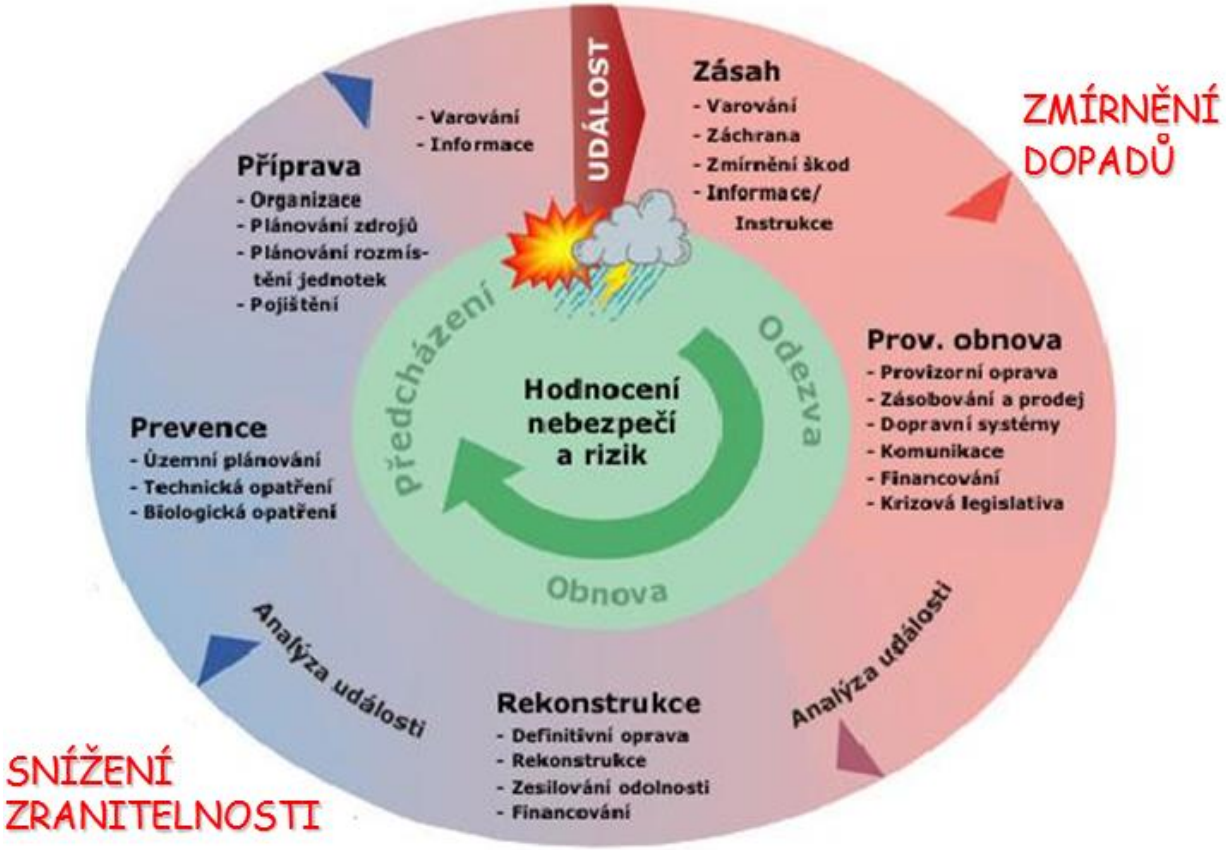
V úvodních podkapitolách jsme se seznámili se všemi manažerskými funkcemi. Rozdělili jsme si je na sekvenční a paralelní (průběžné) funkce. Blíže jsme si jednotlivé manažerské funkce vysvětlili a poukázali na jejich vzájemnou propojenost a návaznost funkcí. Všechny výše zmíněné funkce by měl schopný manažer ovládat. [4]

1.3 Specifika bezpečnostního managementu

Bezpečnostní management reaguje na potřeby lidí, firem, států a organizací za účelem shromažďování poznatků a informací o hrozbách, které na ně mohou působit. Následná rizika naplnění hrozby musí příslušní lidé a systémy vyhodnotit, zpracovat a být schopni tyto rizika minimalizovat, popřípadě je řídit nebo zvládat

Může se jednat o předem definovaný systém, který je schopen na základě vstupních informací (podnětů) reagovat na danou situaci samočinně. Jedná se zejména o aktivační události:

- Poplach - přítomnost nebo vniknutí pachatele
- Sabotáž - například překonání tamperu
- Porucha – systému, napájení…
- Přepadení – aktivace systémů přivolání pomoci
- Vstup / odchod – monitorování osob v objektu (ACS, RFID, heslo…)
- Uzamčení / otevření – dveře, okna, vrata, branky
- Požár – teplota, kouř …



Obr. 6 Mimořádné události [9]

Z výše zmíněného vyplývá, že bezpečnostní management shromažďuje poznatky z:

- policejního managementu,
- krizového řízeni,
- řízení a velení vojenských i civilních operací,
- vnitřní a vnější bezpečnosti,
- bezpečnosti informačních systémů,
- BOZP,
- poznatky všech funkcí a činností bezpečnostních manažerů.

1.3.1 Plánování

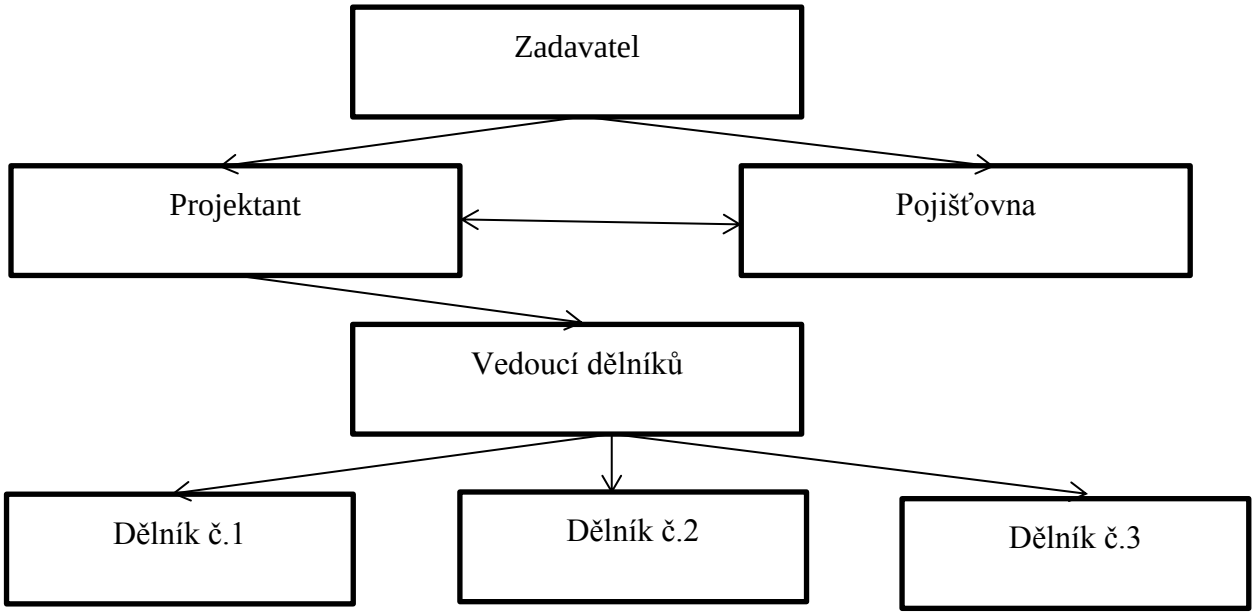
Plánováním z hlediska ochrany majetku rozumíme např.:

Tab. 1 Plánování

Cíl	Způsob dosažení cíle	Zdroje	Odpovědnost
Znemožnění vniknutí pachatele do objektu	Brány, branky, ploty, ostnaté dráty, sirény, fyzická ostraha	Finanční, materiální	Projektant. Osoba, která systém montuje a spravuje.
Zamezení, zmírnění krádeže či chycení pachatele	Projekt a konstrukce systémů (PZTS, MZS, CCTV)	Finanční, materiální	Projektant. Osoba, jež dohlíží na systém jako celek.
Bezpečnost dat	Firewall, silné heslo, Antivirový program	Finanční, materiální	Správce sítě. Uživatel sítě

Po vytyčení daného cíle je nutné, abychom věděli, jak daného cíle dosáhneme, jaké k tomu máme zdroje a zdali je vůbec v našich silách naplnit vytyčený cíl. Pokud ano, máme hotový plán, za který zodpovídá daná osoba.

1.3.2 Organizování



Obr. 7 Ukázka organizování, vlastní zdroj

Organizační struktura, kdy zadavatel chce například zpracovat návrh na bezpečnostní systém v určité třídě zabezpečení, kvůli pojištění majetku.

1.3.3 Kontrola

Z hlediska bezpečnostního managementu kontrolou rozumíme nejčastěji:

- nácvik situací (evakuace, potápěčské cvičení),
- zkoušky sirén,
- simulace mimořádných událostí,
- revize dokumentů,
- revize strojů a zařízení,
- revize BOZP.

1.3.4 Analyzování problémů

V bezpečnostním managementu je analyzování problémů velmi důležité. Proto by ji měli provádět zkušení lidé, někdy i početné skupiny lidí. Na základě správné a včasné analýzy můžeme:

- Zefektivnit včasnost příjezdu jednotek IZS

- Vhodným výběrem zasahujících jednotek minimalizovat následky mimořádné situace
- Minimalizovat úrazy na pracovištích
- Minimalizovat následky způsobené útoky hackerů…

1.3.5 Rozhodování

Rozhodování patří bezesporu k jedné z nejdůležitějších funkcí bezpečnostního managementu. Správně a rychle se rozhodnout v jedné z krizových situací, je hlavním předpokladem k tomu, aby byla daná situace zvládnuta co nejlépe a z co možná nejmenšími následky.

Bezpečnostní management je tedy nedílnou součástí každé organizace a zahrnuje v sobě funkce managementu s důrazem na bezpečnost. Jeho úkolem je tedy dosahovat optimální bezpečnosti řízené organizace pomocí lidí, systémů a technologií. [3]

1.4 Bezpečnost

Bezpečnost je stav, kdy je systém schopen odolávat známým a předvídatelným vnějším a vnitřním hrozbám, které mohou negativně působit proti jednotlivým prvkům, případně celému systému tak, aby byla zachována struktura systému, jeho stabilita a spolehlivost.

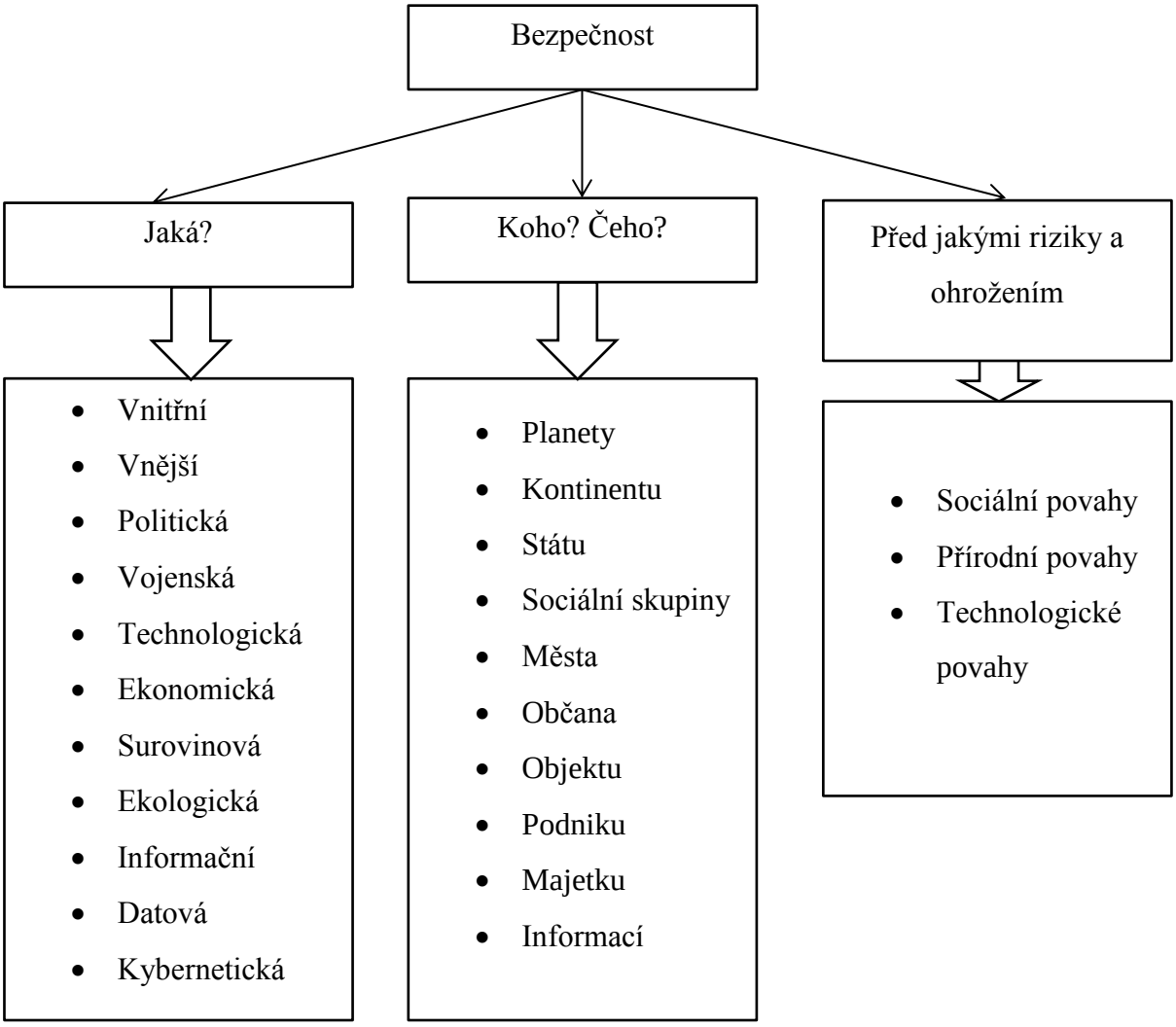
Bezpečnost má základní význam pro:

- Fungování státu
- Existenci člověka jako jedince

Podle Maslowovy pyramidy lidských potřeb je bezpečnost druhou z nejvíce pociťovaných lidských potřeb.

Obr. 8 Maslowova pyramida potřeb, vlastní zdroj

Bezpečnost:



Obr. 9 Dělení bezpečnosti, vlastní zdroj

1.4.1 Hrozba

Hrozba je objektivní skutečnost, která má negativní dopad pro některý chráněný zájem. Závažnost hrozby je úměrná povaze hodnoty a tomu, jak si danou hodnotu ceníme.

Hrozby můžeme dělit na hrozby:

- Neintencionální
- Intencionální

Neintencionální hrozba je jevem přírodním, jako jsou povodně, vichřice, zemětřesení, sopečná činnost, které jsou náhodné povahy. Můžeme je předvídat jen s určitou pravděpodobností.

Intencionální hrozba je zamýšlená. Připravuje ji, spouští a uskutečňuje jedinec, skupina, organizace nebo stát, jako v případě teroristické akce, sabotáže, atentátu nebo válečného aktu.

Z hlediska působení na organizace můžeme hrozby dělit na:

- vnější hrozby,
- vnitřní hrozby.

Vnější hrozby jsou neovlivnitelné, proto můžeme jejich důsledky pouze tlumit. Vnější hrozby dále dělíme na šest oblastí:

- politické hrozby,
- ekonomické hrozby,
- sociální hrozby,
- technologické hrozby,
- legislativní hrozby,
- ekologické hrozby.

Vnitřní hrozby jsou ovlivnitelné. Jejich příčiny můžeme minimalizovat a v některých případech i zcela eliminovat. Dělí se do tří oblastí.

- procesní (projektové) hrozby,
- personální hrozby,
- věcné hrozby.

Je patrné, že z výše uvedeného rozdělení hrozeb vyplývá, že hrozby mohou působit jak na aktiva hmotná tak i na aktiva nehmotná. Současně je ovšem nutné vzít v úvahu, že vnitřní hrozby mohou rovněž působit i vně organizace, a to na aktiva ostatních organizací.

Vlastností hrozby je riziko.[6]

1.4.2 Riziko

Riziko je pravděpodobnost, že dojde k nežádoucí události, ztrátě, která postihne určité cíle, na kterých nám záleží (aktiva). Riziko tedy vzniká působením mezi hrozbou a aktivem. Je

vyjadřováno kombinací pravděpodobnosti výskytu mimořádné události a závažností dopadu na dané aktivum. Riziko je tedy možnost, že s určitou pravděpodobností vznikne událost, která se liší od normálního stavu.

Pro výpočet rizika je použita následující rovnice:

$$Riziko = \frac{(Hrozba) * (Zranitelnost) * (Hodnota)}{Protiopatření} \quad (1)$$

Čím závažnější hrozba, zranitelnost a čím významnější hodnota aktiva, tím je riziko vyšší. Platí zde přímá úměrnost. Naopak čím důkladnější a bezpečnější protiopatření, tím nižší riziko, úměrnost nepřímá.

1.4.3 Riziko X Nejistota

Za hlavní složky rizika jsou považovány nežádoucí následky a nejistota s nimi spojená. Aby se určilo riziko systému, nebo činnosti je nezbytné vyhodnotit oba parametry. Pokud neexistuje jedna ze složek, neexistuje ani riziko. Riziko je tedy kombinací nejistoty a nežádoucích následků, což můžeme shrnout do rovnice:

$$Riziko = Nejistota * Nežádoucí\ následky \quad (2)$$

1.4.4 Riziko X Nebezpečí

Nebezpečí představuje původ (zdroj) rizika. Riziko naopak zahrnuje pravděpodobnost, se kterou tento zdroj může být převeden na skutečné škody. Při použití ochranných opatření je riziko podstatně zredukováno. Riziko totiž závisí nejen na nebezpečí, ale také na ochranných opatřeních přijatých proti nebezpečí. Můžeme napsat rovnici: [6]

$$Riziko = \frac{Nebezpečí}{Ochranná\ opatření} \quad (3)$$

Z rovnice můžeme usoudit, že pokud použijeme dostatečná ochranná opatření, můžeme riziko velmi minimalizovat a naopak.

1.4.5 Bezpečnostní manažeři

Manažera můžeme obecně chápat, jako správce, vedoucího, nebo ředitele. Jedná se tedy o člověka, který řídí určitou skupinu lidí. Ne každý má předpoklady pro to, stát se dobrým

manažerem. Hodnotícím prvkem v práci manažera je bezpochyby práce a výsledky jeho podřízených.

V současné době se manažeři dělí do tří kategorií:

- Vrcholový manažeři,
- Střední manažeři,
- Manažeři první linie.

Existují tři okruhy manažerských dovedností:

- Lidské dovednosti – jsou obecné dovednosti zejména pro provozního manažera, personalistu. Tyto dovednosti jsou důležité pro vedení lidí, motivaci, komunikaci, spolupráci a vzájemné pochopení.
- Technické dovednosti – schopnosti využít specifické vlastnosti, postupy, znalosti techniky, využívat specializované pracovníky. Manažer by měl mít stejné dovednosti technického rázu, jako mají lidí, které řídí.
- Koncepční dovednosti – schopnost vidět věci jako celek (vidět dopředu). Patří sem také schopnost řídit, integrovat a slaďovat zájmy a aktivity podniku.

Další vlastnosti, které by měl manažer zvládat, jsou:

- Vždy jasně vymezit cíle, aby lidé věděli, na čem mají vlastně pracovat,
- Zřetelně vyjadřovat pokyny,
- Jednat s různými typy lidí,
- Rozumět pracovníkům a tolerovat je,
- Rozhodovat se ve složitých situacích,
- Přijímat i poskytovat zpětnou vazbu,
- Dobře organizovat a kontrolovat práci,
- Být schopný přizpůsobit se změnám.[3]

1.5 Řízení rizik

Riziko, jeho řízení, zvládání, ovlivňování nebo minimalizace je v dnešní době stále více používáno a skloňováno. Ať už se jedná o společnost, organizaci popřípadě jedince, vždy jsme vystaveni určitým rizikům, kterým chceme v nejlepším případě zamezit. Avšak to není vždy možné a proto se působící rizika snažíme zmírňovat či řídit.

Obr. 10 Terminologické pojmy k řízení rizik [1]

1.5.1 Aktivum

Do aktiv řadíme všechno, co má pro společnost či jedince nějakou hodnotu. Na základě stanovené hodnoty bychom toto aktivum měli odpovídajícím způsobem chránit. Aktiva můžeme členit do dvou základních kategorií:

- Aktiva hmotná (finanční prostředky, cenné papíry…)
- Aktiva nehmotná (informace, autorská práva…)

Vůči působení hrozby se aktivum vyznačuje určitou zranitelností, která se dá minimalizovat nasazením přiměřených bezpečnostních opatření.

1.5.2 Zranitelnost

Zranitelnost představuje nedostatek, slabinu, které může hrozba využít pro uplatnění svého nežádoucího vlivu. Zranitelnost je vlastností aktiva a vyjadřuje nám, jak je dané aktivum citlivé na působení dané hrozby.

1.5.3 Bezpečnostní opatření

Představuje proces nebo prostředek navržený tak, aby minimalizoval působení rizika, čehož může být dosaženo následujícími opatřeními:

- eliminace zdrojů hrozeb,
- snížením zranitelnosti aktiva,
- snížením pravděpodobnosti výskytu mimořádné události,
- snížením závažnosti dopadu mimořádné události.

Bezpečnostní opatření nám slouží k ochraně aktiva, popřípadě nám umožňují detekci působení hrozeb. V některých případech jsou bezpečnostní opatření schopny těmto hrozbám zcela zabránit nebo je alespoň zmírnit na přijatelnou úroveň. Z pohledu analýzy rizik jsou bezpečnostní opatření charakterizována efektivitou a náklady. Z toho vyplývá, že při návrhu bezpečnostních opatření by neměly vynaložené náklady převyšovat hodnotu námi chráněného aktiva (10-15 % z ceny aktiva).[1]

1.6 Subproces posuzování rizik

Subproces posuzování rizik je jedním z dílčích subprocesů při procesu řízení rizik. Zkládá se z dílčích procesů:

- identifikace rizik,
- analýza rizik,
- hodnocení rizik.

1.6.1 Identifikace rizik

V rámci identifikace rizik provádíme dva základní úkony:

- identifikace aktiv, stanovení hodnoty aktiv a seskupování aktiv,
- identifikaci hrozeb a zdrojů hrozeb.

Cílem identifikace rizik je vytvoření seznamu rizik, která mohou zamezit, snížit či zpomalit dosažení našich cílů. Identifikace rizik by měla být komplexní, je totiž rozhodující pro další nakládání s riziky. Rizika, která v identifikaci nevezmeme v potaz, v dalších krocích nemůžeme eliminovat ani minimalizovat. Protože o nich zkrátka nevíme nebo jsme je opomněli. Proto je při identifikaci rizik důležité vycházet z aktuálních informací. Identifikace tedy zahrnuje všechna rizika, ať už je zdroj daného rizika pod kontrolou nebo není.

Identifikace aktiv tvoří seznam všech aktiv, která nám spadají do procesu řízení rizik. Stanovení hodnoty aktiva vychází z velikosti škody, kterou jeho zničením nebo zcizením dojde. Většinou se při stanovení hodnoty aktiva vychází z:

- nákladových charakteristik (pořizovací cena, reprodukční pořizovací cena),
- výnosových charakteristik (postavení na trhu, know-how, ochranná známka).

Dalším kritériem pro hodnocení aktiv, je uvědomit si zdali se jedná o aktivum:

- jedinečné aktivum,
- snadno nahraditelné aktivum.

Vzhledem k tomu, že aktiv je v dnešní době více a více je vhodné aktiva podobné kvality, ceny a účelu seskupovat brát je jako jedno aktivum. Zde je ale nutné dát pozor na to, aby opatření vzatá na skupinu aktiv jednoho druhu, byla aplikovatelná na všechny aktiva.

Identifikace hrozeb a jejich zdrojů je dělána tím způsobem, že se vybírají ty hrozby a jejich zdroje, které mohou ohrozit minimálně jedno aktivum subjektu. Při identifikaci hrozeb a jejich zdrojů nejčastěji vycházíme z:

- seznamu hrozeb
- vlastní zkušenosti,
- průzkumu,
- předešlé provedené analýzy.[2]

1.6.2 Analýza rizik

Obr. 11 Analýza rizik[9]

Po identifikaci rizik následuje jejich analýza, která poskytuje vstupy pro hodnocení rizik a pro rozhodnutí o tom, zdali je potřebné identifikovaná rizika zvládnou a jakými způsoby je zvládneme. Výsledkem analýzy rizik je tedy stanovení úrovní jednotlivých rizik.

V první fázi analýzy rizik, je analýza hrozeb a zranitelností. Je zřejmé, že každá hrozba se hodnotí vůči danému aktivu či skupině aktiv. U aktiv, kde se očekává působení hrozby, se určí velikost této hrozby k aktivu a také velikost zranitelnosti aktiva k hrozbě.

V dalších fázích analýzy rizik, se stanovují:

- závažnosti dopadu nežádoucí události,
- pravděpodobnosti vzniku nežádoucí události.

Analýzu rizik v závislosti na konkrétním riziku, účelu analýzy a dostupných zdrojích informací provádíme s různou mírou podrobnosti. Analýzu realizujeme:

- kvalitativní způsob,
- semikvantitativní způsob,
- kvantitativní způsob,
- jejich kombinací.

Kvalitativní analýza používá slovního hodnocení k popisu závažnosti potencionálních dopadů a pravděpodobností, s jakou tyto dopady nastanou.

Semikvantitativní analýza používá bodového ohodnocení. Důvodem je vytvoření větší bodové škály, než jak je tomu u kvalitativní analýzy.

Kvantitativní analýza používá číselných hodnot, které jsou mnohem přesnější, než jak je tomu u kvalitativní a semikvantitativní analýze.

Analýza rizik nám tedy slouží k stanovení míry rizika. Na základě ohodnocení aktiv analyzujeme hrozby, u kterých stanovíme míru pravděpodobnosti výskytu. Výsledkem analýzy rizik, je tedy seznam hrozeb. Pro hrozby, které jsou pro organizaci nebezpečné, se navrhuje bezpečnostní opatření, které zvyšuje míru bezpečnosti aktiva.

1.6.3 Hodnocení rizik

Hodnocení rizik je důležité zejména při rozhodování, kdy se rozhoduje, která rizika musí být přednostně řešena. Hodnocení rizik zahrnuje dvě činnosti:

- komparace stanovených úrovní rizika se stanovenými kritérii,
- stanovení přijatelnosti rizika.[7]

Při řízení rizik je nutné míti na paměti, že hrozby působící na organizaci, společnost, objekt nebo jedince působí neustále, mohou se měnit a také se vyvíjet. Proto je nutné subproces posuzování rizik opakovat periodicky, abychom odhalili možná nová rizika. Posuzování rizik je vhodné také provádět při zavádění nových procesů v organizaci.

Je patrné, že rizik působících na organizaci je celá řada a proto je důležité rozhodnou, která rizika je nutné řídit, která stačí minimalizovat na přijatelnou úroveň a která naopak nemusíme brát v potaz, protože jejich účinky na organizaci jsou irelevatní.

2 MAJETEK A JEHO OCHRANA

V době, kdy jsou ve společnosti velké majetkové rozdíly, je nutné si majetek náležitým způsobem chránit. Ochranu majetku můžeme realizovat mnoha způsoby a záleží na nás, jaké náklady k jeho ochraně použijeme. Je nutné mít na paměti, že v případě odcizení námi vlastněného majetku nemusí být prvořadým problémem fyzické odcizení majetku, ale spíše narušení soukromí subjektu, jemuž bylo vniknuto do chráněného prostoru.

Majetek je souhrn veškerých statků, se kterými může majitel volně nakládat a kterými případně může ručit za své závazky.

Majetek dělíme na majetek:

- hmotný,
- nehmotný,
- finanční.

2.1 Hmotný majetek

Hmotný majetek je reprezentován již z jeho názvu hmotným (fyzickým) charakterem. Hmotný majetek dále dělíme podle jeho povahy na majetek:

- nemovitý,
- movitý.

Nemovitý majetek je svázán s půdou, to znamená, že se jedná zejména o pozemky, budovy a jiné vlastněné prostory.

Do movitého majetku řadíme fyzické předměty, jako jsou výrobní stroje, zařízení, automobily nebo materiál.

2.2 Nehmotný majetek

Nehmotný majetek je reprezentován níže zmíněnými položkami:

- zřizovací výdaje,
- nehmotné výsledky výzkumu a vývoje,
- software,
- ocenitelná práva,
- know-how.

2.3 Finanční majetek

Mezi základní rysy finančního majetku jsou vysoká likvidita a bezprostřední obchodovatelnost. Patří zde:

- hotovost,
- ceniny,
- vkladové účty,
- majetkové a dlužné cenné papíry.[10]

2.4 Preventivní činnost při ochraně majetku

Preventivní činnost při ochraně majetku patří k nejdůležitějším činnostem v průmyslu komerční bezpečnosti potažmo v celé bezpečnostní komunitě.

O významu prevence se přesvědčujeme každý den. Preventivní činnost má nepostradatelný význam jak při fyzické ochraně majetku, tak při použití technických prostředků.

Zásady preventivní činnosti jsou:

- včasnost,
- rychlost,
- komplexnost,
- odbornost,
- permanentnost,
- součinnost.

2.4.1 Včasnost

Abychom mohli preventivní činnost hodnotit pozitivně, je třeba ji vykonávat včas. Opatření udělána po uplynutí kritického času potřebného k ochraně majetku jsou zbytečná.

2.4.2 Rychlost

Opatření tkví v tom, že po včasném rozhodnutí o provedení prevence provedeme tato opatření co nejdříve. Opět zde platí, že pokud se rozhodneme opatření udělat později, mohlo by pro nás být zbytečné. Důležitým atributem při tomto opatření je také finanční stránka, na které zpravidla rychlost velmi záleží.[5]

2.4.3 Komplexnost

Jedná se o nasazení všech dostupných opatření v jeden celistvý fungující celek. Jednotlivými opatřeními je myšleno zejména:

- fyzické opatření,
- technická opatření,
- organizační opatření,
- psychologická opatření,
- právně bezpečnostní opatření,
- režimová opatření.

2.4.4 Odbornost

Odbornost je další nepostradatelná činnost, při které nesmíme připustit, aby jakékoliv prevence byla udělána nedbale, neprofesionálně. Prevence by proto měli řídit a vykonávat pouze osoby odborně způsobilé, které mají v dané oblasti teoretické a praktické zkušenosti. Osoby by měli prokazovat odborné vzdělání a zkušenosti v oblastech:

- analytických,
- psychologicko-analytické,
- technické,
- právní,
- pedagogické,
- finanční,
- organizační,
- řídící.

2.4.5 Permanentnost

Permanentnost v preventivních opatřeních spočívá v nepřetržité preventivně výchovné činnosti na všech činnostech, kde hrozí stálé bezpečnostní riziko napadení majetku, které máme za úkol chránit.

Permanentnost má za úkol neustále vyhodnocovat bezpečnostní rizika, provádět analýzy a pomáhat v navrhování a realizování preventivně výchovných opatření k předcházení a zamezení těchto rizik.

2.4.6 Součinnost

Součinnost mezi bezpečnostními komunitami nám zaručuje účinnost a efektivnost prevence. Půjde hlavně o součinnost mezi firmami průmyslu komerční bezpečnosti, soukromými bezpečnostními službami a:

- policií ČR,
- obecní policií,
- ostatními složkami IZS,
- výrobci bezpečnostních technologií a komponentů bezpečnosti ochrany,
- veřejností,
- ostatní místními orgány státní správy a samosprávy.[5]

Cílem prevence je tedy zabránit vzniku mimořádných událostí.

2.5 Fyzická bezpečnost objektu

Fyzická bezpečnost objektu jako stav, vyjadřuje stupeň bezpečí nebo nebezpečí, v němž se referenční objekt nachází z pohledu potenciálního účinku hrozeb fyzickou cestou.

- bankovní instituce,
- objekty spadající do kritické infrastruktury,
- rodinné domy,
- muzea,
- nemocniční zřízení,
- zemědělské plochy,
- a jiné.

Bezpečnost objektu, je dána součtem dílčích ochran či opatření. Propojením a kombinací těchto ochran je pak dosaženo vyšší bezpečnosti objektu. Proto je důležité, aby byly jednotlivé komponenty, režimy a služby vhodně propojeny a navzájem spolu komunikovaly.

Bezpečnost objektu závisí zejména na:

- fyzické ochraně,
- technické ochraně,
- režimové ochraně.

2.5.1 Fyzická ochrana

Fyzická ochrana je činnost člověka či skupiny lidí, která je schopna poskytnou svými zákroky, které vedou k odvrácení nebezpečí nebo ke snížení následků vzniklých působením hrozeb, ochranu majetku i osob. Aktivně se podílí na eliminaci a minimalizaci záměrů narušitele a je schopna vynaložit bezprostřední opatření k jeho dopadení. Nejčastěji se jedná a vyškolené zaměstnance hlídacích služeb.

Patří k nejstarší a nejčastější formě ochrany majetku a osob. Zdali je prováděna odborně a precizně, bývá nejjednodušší a nejefektivnější. Její velkou výhodou je, že lze v případě nutnosti provést okamžitý zásah vedoucí k ochraně majetku a osob, čímž může zamezit případnému hrozícímu nebezpečí, popřípadě ho minimalizovat.

Fyzickou ochranu chápeme jako určitou formu dohledu nad:

- zákazníky,
- zbožím,
- personálem,
- veškerá námi důležitá aktiva.

Mezi hlavní úkoly fyzické ochrany patří především:

- Dozor nad veřejným pořádkem a bezpečnostní dohled,
- Převoz hotovosti a cenin,
- Hlídková činnost uvnitř i vně budovy,
- Kontrola dodržování režimových opatření,
- Kontrola osob, vozidel a zavazadel.

Fyzická ochrana se dělí do následujících kategorií:

- Ochrana podle časového rozvrhu,
- Ochrana podle druhu výkonu,
- Podle způsobu zajištění ochrany,
- Podle výstroje a výzbroje.

Fyzická ochrana patří mezi základní prvky ochrany. Důležitou roli zde hraje zkušenost získaná jedincem či skupinou lidí. V některém odvětví fyzické ochrany jsou získané zkušenosti téměř to nejdůležitější, co je vyžadováno (např. přeprava cenin a hotovostí a bodyguarding).

2.5.2 Technická ochrana

Technická ochrana zajišťuje bezpečnostními prvky, jejichž použitím se zabraňuje, ztěžuje nebo oznamuje narušení objektu.

Využívá technických prvků používaných v průmyslu komerční bezpečnosti:

- Mechanických prvků,
- Elektronických, elektrických prvků,
- Smíšených, speciálních prvků.

Mechanická ochrana je ochrana majetku s využitím mechanických prvků, prostředků či systémů, které jsou konstruovány tak, aby pachateli zamezily nebo znesnadnily proniknutí do chráněného objektu. Jedná se o prvky nebo systémy, které pro svou činnost nejsou závislé na elektrické energii, ale jsou založeny na fyzikálních vlastnostech, zejména na mechanické pevnosti materiálu.

Mezi mechanickou ochranu řadíme mechanické zábranné systémy:

- perimetrické ochrany,
- plášťové ochrany,
- prostorové ochrany,
- předmětové ochrany.

Elektronická nebo také elektrická ochrana je ochrana s využitím elektrických a elektronických prvků, tedy prvky, které pro svou činnost potřebují dodání elektřiny, ať už ze sítě nebo z akumulátorů. Tyto zařízení slouží zejména k monitorování (zboží, objektu, osob…), ohlášení nežádoucího stavu na DPPC nebo DPC a patří, jsem:

- Poplachové zabezpečovací systémy (PZS)
- Elektrická požární signalizace (EPS)
- Uzavřené střežící a dohlížecí televizní okruhy (CCTV)
- Přístupové systémy (ACS)
- Satelitní vyhledávání vozidel
- Elektronická ochrana zboží
- Ochrana dat a informací

Smíšená ochrana majetku využívá kombinaci mechanických zábranných systému a elektronickou ochranu jako jednotlivý celek. Patří sem například elektronické blokování dveří a závor nebo kombinované elektromechanické zámky a zámkové systémy.

2.5.3 Režimová ochrana

Je soubor procedur a opatření, které zahrnují režim vstupů a výstupů osob, vjezdu a výjezdu vozidel do chráněného prostoru.

V souladu se zákony a potřebami organizace řeší, jakým způsobem budou lidé postupovat při ochraně podniku. Režimovým opatřením rozumíme:

- Administrativní uspořádání
- Organizační uspořádání
- Věcné uspořádání

Vztahů mezi lidmi, jejich činnostmi a vlastními procesy v oblasti výkonu i řízení za účelem sladění všech prvků a s cílem dosáhnout harmonického stavu v dané organizaci. V rámci režimové ochrany jsou v organizaci také klasifikovány informace z hlediska jejich citlivosti nebo důvěrnosti.

Režimová opatření upravují:

- Činnost lidí uvnitř organizace
- Pohyb a chování přicházejících osob
- Výstup informaci, dat a dokumentů z podniku [5]

3 METODY ANALÝZY RIZIK

Cílem analýzy rizik je posouzení aktuálních nedostatků s vyčíslením potenciálních ztrát, které mohou tyto nedostatky způsobit.

Analýzami rizik rozumíme jednodušší ekonomické analýzy ztrát způsobené například výpadkem výrobního zařízení, až po složité modely úniku nebezpečných látek a radioaktivity do jednotlivých složek životního prostředí.

Výběr vhodné metody pro posouzení rizik je velmi důležitým předpokladem k tomu, aby byla analýza rizik správně a objektivně udělána. Každá z metod má jiné použití. Rozdíly mezi analýzami rizik jsou následující:

- velikost a složitost procesu,
- různé druhy výsledků,
- náročnost na pracovní tým a čas.[NORMA]

Některé metody na sebe navazují nebo se i překrývají, jiné jsou zase naprosto nesrovnatelné. Využívá se velkého množství metod, ale jako stěžejní metody jsou považovány zejména tyto:

- **Srovnávací metody:**
  - Indexové metody RR
  - Revize bezpečnosti SR
  - Kontrolní seznam CL
- **Analytické metody založené na deterministickém přístupu**
  - Předběžná analýza ohrožení PHA
  - What if analýza WI
  - Analýza nebezpečnosti a provozovatelnosti HAZOP
  - Analýza příčin a následků poruch FMEA
  - Analýza stromem poruch FTA
  - Analýza stromem událostí ETA
  - Analýza příčin a následků CCA
  - Analýza lidského faktoru HRA
- **Analytické metody založené na pravděpodobnostním přístupu**
  - Analýza stromem poruch (FTA) kvantitativní
  - Analýza stromem událostí (ETA) kvantitativní

- Blokové diagramy (BD)
- Markovy řetězce (MCh)[Norma]

3.1 Srovnávací metody

Srovnávací metody jsou zaměřeny na identifikaci zdrojů rizika. Většinou se provádějí na základě porovnávání a aplikování provozních zkušeností získaných z provozu nebezpečných zařízení a doplněné prohlídkou zařízení. Jejich cílem je odhalení slabin nebezpečného zařízení.

3.1.1 Indexové metody (RR – Relative Ranking)

Jedná se o metody rychlého posuzování bezpečnosti procesu s využitím indexů pro oceňování nebezpečných vlastností procesu. Bezpečnost procesu se hodnotí podle indexu pro toxicitu látek a indexu pro požár a výbuch do tří kategorií nebezpečnosti. Princip metod je bodové ohodnocení jednotlivých operací procesu a procesních podmínek na základě stanovených výpočtů. Analýzu provádí jeden nebo více analytiků. Časový interval by neměl přesáhnout dva týdny a je závislý na velikosti a složitosti provozu. Indexových metod existuje celá řada, ale v podstatě jsou si velmi podobné:

- Dow Fire and Explosion Index (F&EI) – metoda pro posuzování nebezpečí požáru a výbuchu u procesních jednotek
- Mond Index – metoda posuzuje kromě požáru a výbuchu i toxicitu látek
- Rapid Ranking – metoda identifikující nebezpečí požáru a výbuchu a také ohrožení toxickou látkou
- Substance Hazard Index (SHI) – metoda klasifikující nebezpečnost látek porovnáním prudce toxické koncentrace látky ve vzduchu a rovnovážné koncentrace látky za normální teploty
- Material Hazard Index (MHI) – metoda stanovuje přípustné limitní množství nebezpečné látky z hlediska bezpečnosti provozu
- Chemical Exposure Index (CEI) – metoda pro posouzení ohrožení toxickou látkou
- Threshold Planning Quantity Index (TPQ) – metoda určující přípustné limity množství látky, při překročení musí být provedena bezpečnostní opatření
  [**BTSM II**]

Indexové metody nám slouží k posuzování a identifikaci rizik, které mohou vzniknout požárem, výbuchem nebo toxicitou nátek. Proto jsou indexové metody vyvíjeny nejčastěji

chemickými společnostmi pro určité specifické procesy. Pokud jsou indexové metody dobře provedeny, mohou pomoci k včasnému zásahu ještě před vznikem nežádoucí situace a tím snížit újmu na životech, zdraví a majetku.

3.1.2 Revize bezpečnosti (SR – Safety Review)

Neboli bezpečnostní prohlídka byla první technika použita pro identifikaci zdrojů rizika. Pro stávající zařízení je obvykle prováděna z inspekčních pochůzek, které se mohou lišit:

- informační pochůzky,
- rutinní vizuální prohlídky,
- přesné, metodické a týmové prohlídky.

Revize bezpečnosti je určena pro identifikaci podmínek nebo provozních činností v podniku, které by mohly vést k nehodě a následně ke zranění, významné újmě na majetku či na životním prostředí. Revize bezpečnosti zahrnuje rozhovory s mnoha lidmi v podniku napříč celou organizační strukturou podniku. Na základě zjištěných informací je revizor bezpečnosti schopen vytvořit odhad možných situací a scénářů, které mohou způsobit újmu. Základem pro provádění bezpečnostních prohlídek je zkušenost. Náročnost studie se pohybuje od jednoho do několika týdnů.

3.1.3 Kontrolní seznam (CL – Checklist Analysis)

K analýze kontrolním seznamem se používá psaný seznam položek nebo kroků k ověření stavu systému. Kontrolní seznam poskytuje základ pro zhodnocení procesních zdrojů rizika. Měl by odhalit problémy, které vyžadují pozdější podrobnou analýzu. Obecné kontrolní seznamy proto bývají často kombinovány s jinou z technik na identifikaci zdrojů rizika. Mnohdy bývá kontrolní seznam používán s what If analýzou.

Využívá se často při projektování jako kontrola souladu se standardními podmínkami.

Obr. 12 Kontrolní seznam[11]

Kontrolní seznam má široké uplatnění v mnoha oblastech ochrany majetku. Na základě existující kontrolního seznamu se provádí kontrola, zdali byla činnost, stav, proces proveden podle příslušných norem, směrnic či vyhlášek. Je důležité, aby se při inovaci procesů, zavádění nových činností aktualizoval také kontrolní seznam.

Srovnávací metody upozorňují na nebezpečné části hodnoceného zařízení. Avšak nejsou schopny číselně vyčíslit pravděpodobnost selhání dílčích systémů. Nejsou schopny definovat podíl jednotlivých částí nebezpečného zařízení na vzniku pravděpodobnosti nebezpečné události. Pomocí srovnávacích metod nelze vyčíslit míru rizika.

3.2 Analytické metody založené na deterministickém přístupu

Jsou metody zaměřené na identifikaci zdrojů rizika. Analyzují příčiny vzniku nebezpečných událostí a scénáře rozvoje nebezpečné události. Pro definované nebezpečné události se vytváří seznam poruch systémů, komponent a chyb obsluhy, které k těmto událostem vedou. Výsledky dávají dobrou představu o chování nebezpečného zařízení. Avšak neumožňují stanovit pravděpodobnost výskytu nebezpečných jevů, pravděpodobnosti selhání pro bezpečnost důležitých komponent, systémů a zásahů obsluhy.

3.2.1 Předběžná analýza ohrožení (PHA – Preliminary Hazard Analysis)

Jedná se o metodu vyvinutou pro hodnocení bezpečnosti v armádě USA. V průmyslu má využití zejména při návrhu projektu zařízení, ale lze ji použít i na stávající zařízení. Metoda nám umožňuje poměrně jednoduchým způsobem identifikovat ohrožení ještě před samotnou výstavbou zařízení a tím přispět k minimalizaci nákladů na případné změny. Z výše zmíněného nám tedy vyplývá výhoda PHA analýzy, která tkví ve včasném seznámení všech pracovníků s možnými druhy nebezpečí procesu a zvládnutí bezpečnosti od počátku života zařízení.

Mezi potenciální ohrožení většinou patří:

- požár,
- exploze,
- toxicita,
- koroze,
- vibrace,
- mechanická porucha,
- a další…

Po identifikaci nebezpečí se vyhodnocují možné příčiny a následky nehod a výsledkem je zařazení do jedné ze čtyř kategorií nebezpečí:

1. Zanedbatelné
2. Obvyklé
3. Závažné
4. Katastrofické nebezpečí

Klasifikace nám slouží zejména pro určení priorit při snižování ohrožení. Výsledky se mohou zapisovat do tabulky, která obsahuje identifikovatelné nebezpečí, příčiny a následky nehod, kategorii nebezpečí a doporučené opatření. Analýzu může provádět jeden ale i více analytiků, časová náročnost se pohybuje podle náročnosti mezi jedním až třemi týdny.

Metoda PHA má v počáteční fázi technického života procesu dvě základní přednosti:

- Identifikace potenciálního nebezpečí v počáteční fázi technického života procesu, kdy případná korelace vyžaduje minimální náklady nebo narušení provozu

- Podpora práce vývojového týmu při vypracování souboru provozních předpisů, které budou používány v průběhu technického života zařízení

3.2.2 What if analýza (WI)

What if analýza je jednoduchá analytická technika používaná při rozhodování a řízení rizik. Její princip je založen na hledání možných dopadů vybraných situací. V podstatě se jedná o strukturovaný brainstorming, kde se v rámci diskuse hledají:

- Dopady konání či procesů
- Opatření proti těmto dopadům

Zpravidla se analýzy účastní skupina zkušených lidí, která klada otázky nebo možné dopady pomocí otázek „co se stane když…“. Jedná se o velmi flexibilní analýzu, která se může přizpůsobit konkrétnímu účelu. Jejím cílem je identifikace problémů nebo nebezpečných stavů v procesu. Postup what if analýzy by měl být následující:

- Definování oblasti zájmu,
- Definování cílových zájmů problému,
- Generování otázek (když),
- Generování odpovědí (co se stane),
- Generování opatření na vzniklé situace.

Obr. 13 Ukázka analýzy what if, s principem brainstormingu[12]

Využití What if analýzy je zcela univerzální a jejím výstupem je popis potencionálních problémů nebo rizik včetně doporučení, jak jim předcházet.

Vzhledem ke komplexnosti metody, při generování vhodných otázek co když, je metoda vhodná nejen do všech odvětví oblasti ochrany majetku, ale téměř všude, kde je nutné řešit určitý problém..

3.2.3 Analýza nebezpečnosti a provozovatelnosti (HAZOP – Hazard and Operability Analysis)

Metoda HAZOP byla vytvořena jako nástroj k systematické podrobné analýze bezpečnosti složitého technologického zařízení, nejčastěji v odvětvích se spojitou či vsádkovou výrobou. Umožňuje identifikovat nebezpečné stavy, které se na zařízení mohou vyskytnout, najít kritická místa (prvky) systému a následně vyhodnotit riziko. Hlavním cílem je identifikovat možné nebezpečné stavy.

V chemickém průmyslu je důležité určení zdrojů rizika a určení příčin spolu s možnými scénáři nehod, které mohou vyústit v závažnou havárii. Zejména pro určení příčin a odhad možných následků (generování havarijních scénářů) je nezbytné použít detailní analýzu technologických zařízení, kdy je cílem najít a ocenit možné zdroje rizika.

Analýza metodou HAZOP probíhá v následujících krocích:

- odhalení příčin,
- odhad možných následků,
- návrhy opatření,
- ocenění.

Principem je generování odchylek od projektového stavu. Odchylky se generují připojením klíčového slova. Tímto způsobem je možné vygenerovat téměř všechny odchylky, které mohou třeba jen teoreticky nastat.

Klíčová slova jsou:

Tab. 2 Ukázka klíčových slov pro metodu Hazop [13]

Klíčové slovo	**Logický význam**	**Příklad**
NENÍ	plná negace původní funkce	není médium v zásobníku
VĚTŠÍ	kvantitativní nárůst	větší teplota v zásobníku
MENŠÍ	kvantitativní pokles	menší teplota v zásobníku
A TAKÉ, JAKOŽ I	kvalitativní nárůst (výskyt ještě jiného případu)	průnik chladicí vody do média v reaktoru
A ROVNĚŽ	kvalitativní nárůst	zanášení topného hadu
ČÁSTEČNĚ	kvalitativní pokles	nepřítomnost některé složky
REVERZE	opačná funkce (činnost)	reverzní tok média ve výměníku
JINÝ	úplná náhrada	jiné médium v koloně
PŘEDČASNÝ	předčasná funkce (činnost)	–
ZPOŽDĚNÝ	opožděná funkce (činnost)	–

Důvody používání metody HAZOP:

- Jedná se o uznávanou a léty ověřenou metodu
- Výstupem není jen identifikace nebezpečných stavů, ale také návrh opatření
- Systematická metoda
- Vyvinuta na základě poznatků z praxe
- Široká možnost využití

Naproti tomu je však analýza prováděná metodou HAZOP náročná na čas, znalosti a zkušenosti těch, kdo ji vypracovávají.

Metoda HAZOP se používá zejména v chemickém průmyslu a to na velké i malé technologické celky.[13]

3.2.4 Analýza příčin a následků poruch (FMEA – Failure Mode and Effect Analysis)

Jedná se o metodu používanou zejména v předvýrobních etapách na preventivní odstranění možných závad a chyb. Tato metoda pomáhá identifikovat nejkritičtější a nejpravděpodobnější chyby ve výrobku nebo v procesu. Umožňuje rozeznat v různých fázích návrhu výrobků nebo procesů co nejdříve možnosti vzniku poruch, určit jejich možné následky, ohodnotit rizika a bezpečně jim předejít.

Pomocí analýzy FMEA jsou identifikovány:

- všechny možné způsoby poruch různých částí systému,
- důsledky, jaké mohou mít tyto poruchy na systém,
- mechanismy poruch,
- způsoby, jak zabránit poruchám anebo zmírnit důsledky poruch na systém.

Existuje několik aplikací analýzy FMEA:

- FMEA návrhu (nebo produktu), která se používá pro součásti a produkty,
- FMEA systému, která se používá pro systémy,
- FMEA procesu, která se používá pro výrobní a montážní procesy,
- FMEA služby,
- FMEA softwaru.

Analýza FMEA může být použita k následujícím činnostem:

- pomoc při volbě alternativ návrhu s vysokou spolehlivostí,
- zajištění, aby byly zohledněny všechny druhy poruch systémů, procesů a jejich důsledků na provozní úspěch,
- identifikují se v ní způsoby a důsledky lidské chyby,
- poskytuje základnu pro plánování zkoušek a údržby fyzických systémů,
- zlepšuje návrh postupů a procesů.

Mezi silné stránky metody FMEA patří:

- Jsou široce aplikovatelné na způsoby poruch činnosti člověka, na způsoby poruch zařízení, systému a na hardware, software a postupy.
- Identifikují se při nich způsoby poruch součástí, jejich příčiny a jejich důsledky pro systém.

- Vyhýbají se potřebě nákladných modifikací zařízení uvedených do provozu pomocí časné identifikace problémů v etapě návrhu.
- Identifikují se způsoby jednobodových poruch a požadavky na zálohované nebo bezpečnostní systémy.

K jejich omezením patří:

- Analýzy mohou být použity pouze k identifikaci jednotlivých způsobů poruch, ne ke kombinaci způsobů poruch.
- Studie mohou být časově náročné a nákladné, nejsou-li adekvátně řízeny a není-li na ně zaměřena dostatečná pozornost.
- U složitých systémů mohou být obtížné a zdlouhavé.

Jak již bylo zmíněno analýzu FMEA je možné použít do řady aplikací. Jedná se o metodu, které může včasně zabránit vzniku nebezpečné situace a tím minimalizovat množství způsobených škod.

3.2.5 Analýza stromem poruch (FTA – Faul Tree Analysis)

Jedná se o techniku sloužící k identifikaci a analýze faktorů, které mohou přispívat ke specifikované nežádoucí události (vrcholová událost). Faktory jsou identifikovány deduktivně, jsou organizovány logickým způsobem a jsou znázorněny pomocí obrázků v diagramu stromu, který zobrazuje příčinné faktory a jejich logický vztah k vrcholové události.

K faktorům identifikovaným ve stromu se mohou řadit události, které souvisí s poruchami součástí hardwaru, lidskými chybami nebo s jakýmikoliv jinými příslušnými událostmi, které vedou k nežádoucí událostí.

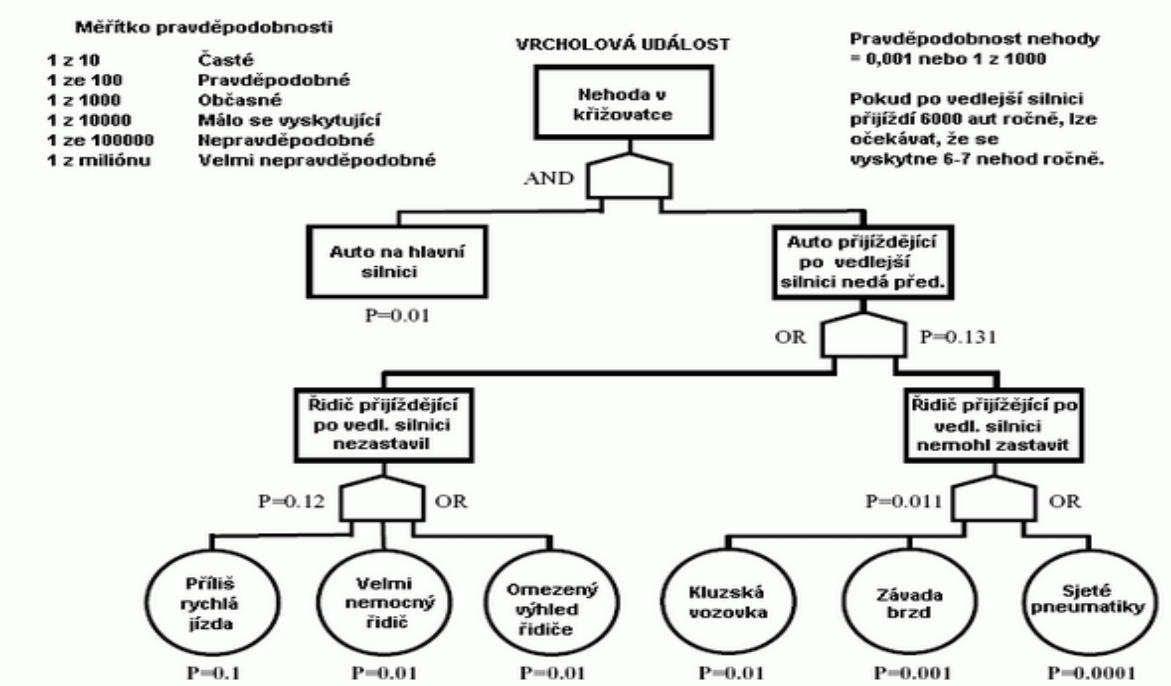
Analýza stromem poruch se může použít kvalitativně s cílem identifikovat možné příčiny a cesty vedoucí k poruše, nebo kvantitativně s cílem vypočítat pravděpodobnost vrcholové události, za předpokladu, že jsou známy pravděpodobnosti příčinných událostí.

Může se použít v etapě návrhu systému s cílem identifikovat potenciálně možné příčiny poruchy a tudíž volit mezi různými variantami návrhu. Může se použít v etapě provozu s cílem identifikovat, jakým způsobem může dojít k významné poruše a určit relativní důležitost různých cest vedoucích k vrcholové události. Může se také použít k analýze

poruchy, ke které došlo, s cílem graficky znázornit způsob, jakým se různé události setkaly, aby způsobily poruchu.

Mezi silné stránky FTA patří:

- Přináší disciplinovaný přístup, který je vysoce systematický, ale zároveň dostatečně flexibilní, aby umožnil analýzu rozdílných faktorů včetně interakcí a fyzických jevů.
- Pozornost je zaměřena na ty důsledky poruch, které se přímo vztahují k vrcholové události.
- Analýza FTA je užitečná zejména při analýze systému s mnoha rozhraními a interakcemi.
- Grafické znázornění vede ke snadnému pochopení chování systému a zahrnutých faktorů, ale jelikož jsou stromy často rozsáhlé, může zpracování stromů poruch vyžadovat počítačové systémy.



Obr. 14 Metoda FTA [8]

K jejich omezení patří:

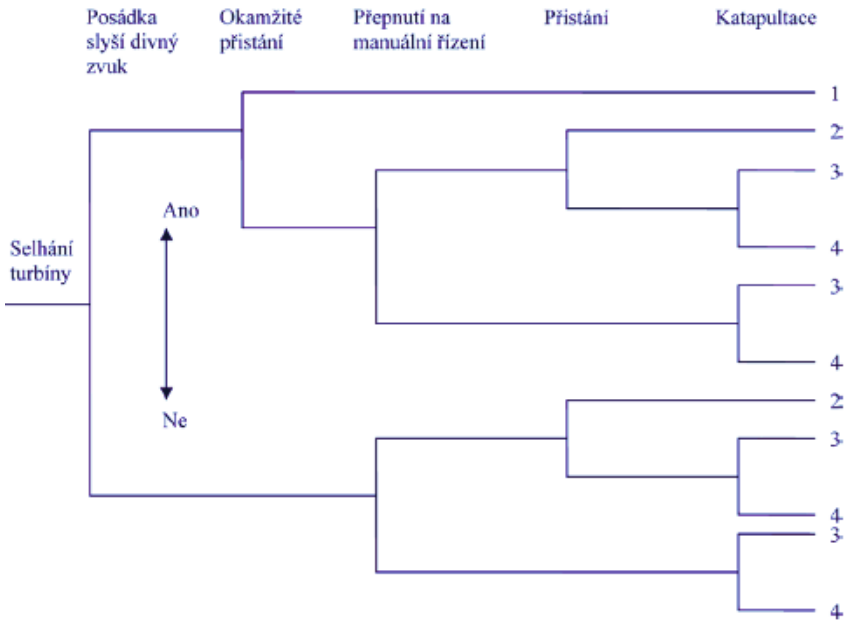
- Ve výpočtech pravděpodobností vrcholové události jsou zahrnuty nejistoty v pravděpodobnostech základních událostí. Výsledkem toho může být vysoký stupeň nejistoty tam, kde pravděpodobnosti poruch základních události nejsou přesně známy. Avšak u dobře pochopeného systému je možné dosáhnout vysoké míry důvěry.
- V některých situacích nejsou příčinné události provázané a může být obtížné zjistit, zda jsou obsaženy veškeré důležité cesty vedoucí k vrcholové události.
- Strom poruch je statický model, pozornost není zaměřena na vzájemné časové závislosti
- Strom poruch se může zabývat pouze binárními stavy
- Strom poruch neumožňuje, aby do něho byly snadno začleněny domino efekty nebo podmíněné poruchy [8]

3.2.6 Analýza stromem událostí (ETA – Event Tree Analysis)

Analýza stromem událostí je grafická technika sloužící k prezentaci vzájemně se vylučujících sledů událostí, které následují po iniciační události podle fungování/nefungování různých systémů navržených k tomu, aby zmírnily následky dané události. Technika může být použita jak kvalitativně tak kvantitativně.

Analýza ETA se používá zejména k modelování, výpočtu a klasifikaci různých nehodových scénářů, které následují po iniciační události.

Analýza ETA může být použita v jakékoli etapě životního cyklu produktu nebo procesu. Může být použita kvalitativně s cílem pomoci při brainstormingu o možných scénářích a sledech událostí, které následují po inicializační události a o způsobu, jak na výsledky působí různá ošetření, bariéry nebo prvky řízení rizika, jejichž cílem je zmírnit nežádoucí výsledky.



Obr. 15 Metoda ETA[8]

Mezi silné stránky ETA patří:

- Analýza ETA znázorňuje jasným schematickým způsobem možné scénáře následující po iniciační události, které jsou analyzovány a ukazuje vliv úspěchu nebo poruchy.
- Vysvětluje časování, závislosti a domino efekty, které jsou pro modelování ve stromech poruch těžkopádné
- Graficky znázorňuje sledy událostí, které není možné zobrazit při použití stromu poruch

K jejich omezení patří:

- Aby byla analýza ETA použita jakožto součást vyčerpávajícího posuzování, je třeba identifikovat veškeré možné iniciační události.
- Pomocí stromů událostí je možné se zabývat pouze stavy úspěchu nebo poruchy systému a je obtížné začlenit opožděné události úspěchu nebo obnovy[8]

3.2.7 Analýza příčin a následků (CCA – Cauce – Consequence Analysis)

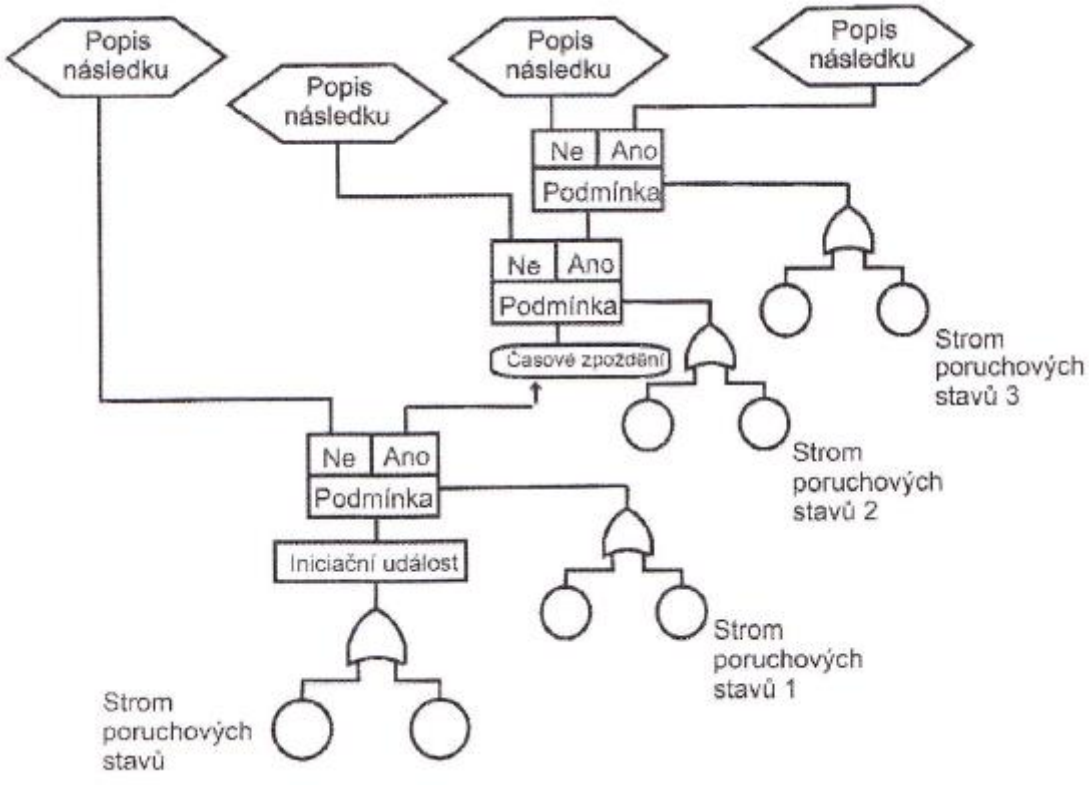
Analýza příčin a následků je kombinací analýzy stromů poruch a analýzy stromu událostí. Začíná kritickou událostí a pomocí ní jsou analyzovány následky s využitím kombinace

logických hradel ANO/NE, která znázorňují podmínky, které mohou nastat nebo poruchy systémů navržených ke zmírnění následků iniciační události. Příčiny podmínek poruch jsou analyzovány pomocí stromů poruch.

Metoda je používána k analýze různých cest, kterými by se systém ubíral po tom, kdyby nastala kritická událost a v závislosti na chování určitých subsystémů. Jsou-li cesty kvantifikovány, poskytnou odhad pravděpodobnosti různých možných následků, které následují po kritické události.

Jelikož každý sled v diagramu příčin a následků je kombinací dílčích stromů poruch, může být analýza vztahu příčin a následků použita jako nástroj pro vytvoření velkých stromů poruch.

Vytvořit a použít diagramy je složité a je tendence použít je v situaci, kdy je intenzivní



Obr. 16 Metoda CCA[8]

úsilí odůvodněno velikostí možného následku poruchy.

Výhoda analýzy příčin a následků je stejná jako výhody kombinace stromů událostí a stromů poruch. Navíc tato analýza překonává omezení těchto technik tím, že je pomocí ní

možné analyzovat události, které se vyvíjejí v čase. CCA analýza poskytuje vyčerpávající pohled na systém.

Analýza příčin a následků má své uplatnění všude, kde je třeba řešit složité systémy a snižovat jejich poruchovost. Jedná se zejména o odvětví:

- Energetiky
- Vědeckého výzkumu
- Letectví

3.2.8 Analýza lidského faktoru (HRA – Human Reliability Analysis)

Analýza lidského faktoru se zabývá dopadem činností člověka na funkčnost systému a může být použita k hodnocení vlivů lidské chyby na systém.

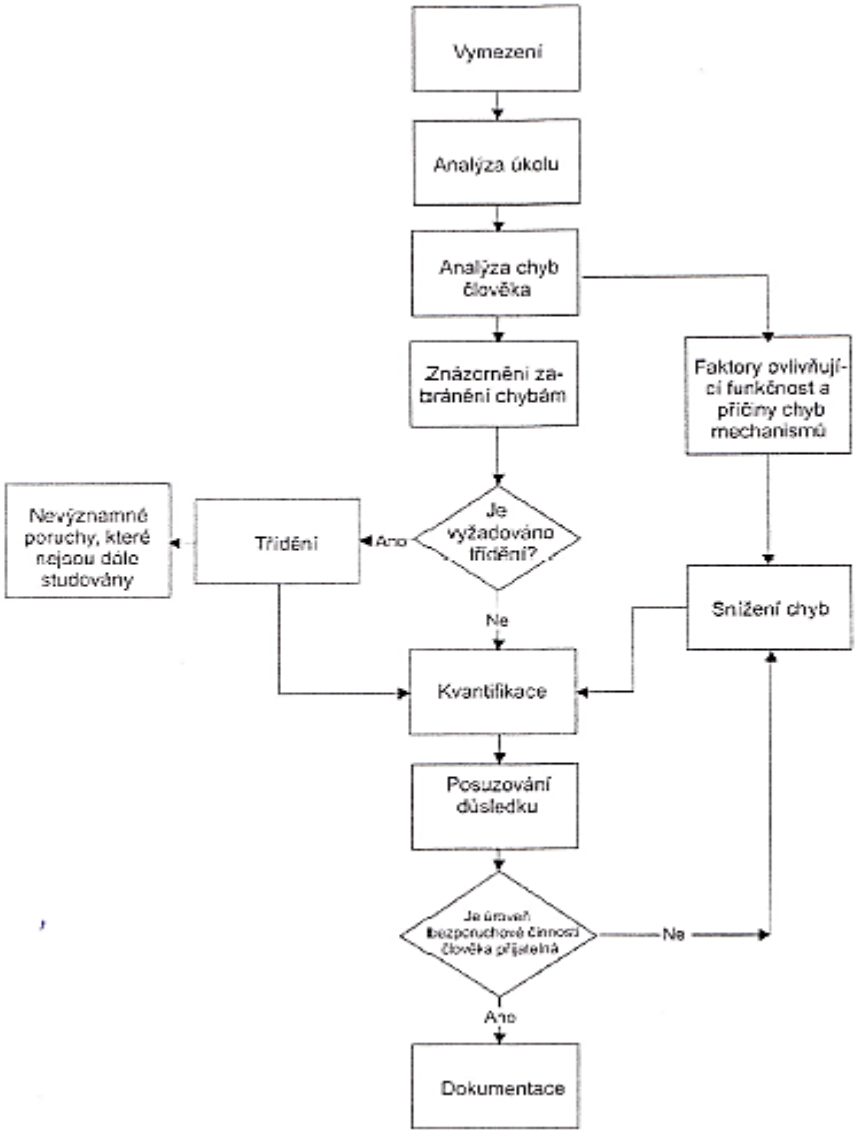
Mnoho procesů v sobě zahrnuje potenciál lidské chyby, zejména v případě, kdy je doba, kterou má provozovatel k dispozici na to, aby učinil rozhodnutí, krátká. Pravděpodobnost, že se problémy rozvinou natolik, aby se staly závažnými, může být malá. Občas však lidský zásah může být jedinou obranou, jak předejít počáteční poruše.

Mezi silné stránky HRA patří:

- Poskytuje formální mechanismus k začlenění lidské chyby do úvah o rizicích souvisejících se systémy, kde lidé často hrají důležitou roli
- Formální zohlednění způsobů a mechanismů lidských chyb může pomoci při snížení pravděpodobnosti poruchy v důsledku chyby

K jejich omezení patří:

- Složitost a rozmanitost lidí, což způsobuje, že je obtížné stanovit jednotlivé způsoby pravděpodobnosti poruch
- Mnoho činností lidí není možné popsat jednoduchým způsobem. Metoda HRA má problém se vypořádat s částečnými poruchami, poruchami v kvalitě, nebo špatným rozhodováním [8]



Obr. 17 Metoda HRA, vlastní zdroj[8]

3.3 Analytické metody založené na pravděpodobnostním přístupu

Jedná se o skupinu metod, které jsou schopny hodnotit rizika číselně. Obdobně jako při deterministickém přístupu se na základě provedených analýz vzniku a rozvoje nebezpečné události sestavuje seznam všech primárních jevů, které samostatně či v kombinacích vedou ke vzniku nebezpečné události. K primárním jevům jsou dále přiřazeny pravděpodobnosti jejich výskytu a vypočítává se pravděpodobnost vzniku nežádoucí události. Mezi nejznámější a nejpoužívanější patří:

- Analýza stromu poruch (FTA) - kvantitativní
- Analýza stromu událostí (ETA) - kvantitativní

- Blokové diagramy (BD)
- Markovy řetězce (MCh)

Uvedené metody tedy mohou přesně vyčíslit pravděpodobnost vzniku nebezpečné události. Je ale nutné znát pravděpodobnosti dílčích jevů a možných poruch vzniklých opotřebením, vadou nebo lidskou chybou. Děje se tak na základě sledování poruchovosti systémů, komponent a omylů lidského činitele, za pomocí matematicko-statistických metod.

V kapitole byli uvedení vybrané metody analýzy rizik, jejich bližší popis, oblasti jejich hlavního použití, co patří k jejich přednostem a co k jejich omezení.

II. PRAKTICKÁ ČÁST

4 IMPLEMENTACE VYBRANÝCH METOD ANALÝZY RIZIK V OBLASTI OCHRANY MAJETKU

Možnosti využití metod analýz rizik v oblasti ochrany majetku je velmi široké. Mezi hlavní oblasti patří:

- Fyzická bezpečnost objektu
- Proces zřizování poplachových zabezpečovacích a tísňových systémů (PZTS)
- Proces zřizování elektronické požární signalizace (EPS)
- Převoz cenin a peněžní hotovosti

4.1 Fyzická bezpečnost objektu

Fyzická bezpečnost patří mezi nejstarší typy ochrany. Obvykle je realizována klasickými stavebními prvky, mechanickými zábrannými systémy a s rozvojem bezpečnostních technologií také systémy elektronickými.

Úkolem fyzické bezpečnosti je zabezpečit referenční objekt aby dosahoval požadované míry bezpečnosti. Míra bezpečnosti se bude lišit vzhledem k důležitosti chráněným aktivům, které se v referenčním objektu nachází (peníze, starožitnosti, utajované informace, léky, jedy, chemikálie).

Mezi základní hrozby z pohledu fyzické bezpečnosti jsou:

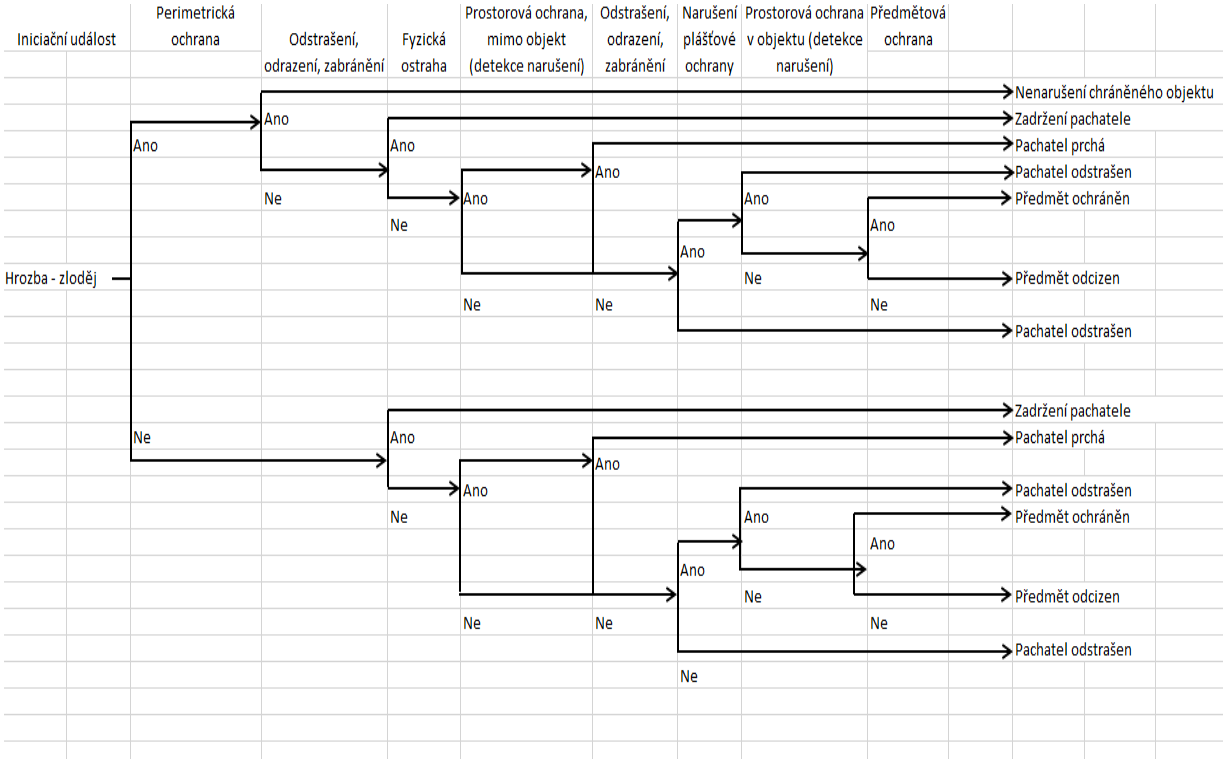
- Kriminalita
- Teroristický útok
- Vojenský zásah cizí moci

Kriminalita

Vzhledem k tomu že se zabývám fyzickou bezpečností objektu, bude zde kriminalita reprezentována pachatelem, jenž se snaží dostat do námi chráněného objektu.

Je zřejmé, že kriminalita a také úroveň pachatele (zručnost, zkušenost, technické vybavení) bude na území České republiky různá. Pomocí statistik, jež si Policie ČR vede, je pak vhodné daná opatření přizpůsobit danému hraji či lokalitě.

4.1.1 Použití analýzy stromem událostí



Obr. 18 Analýza stromem událostí, vlastní zdroj

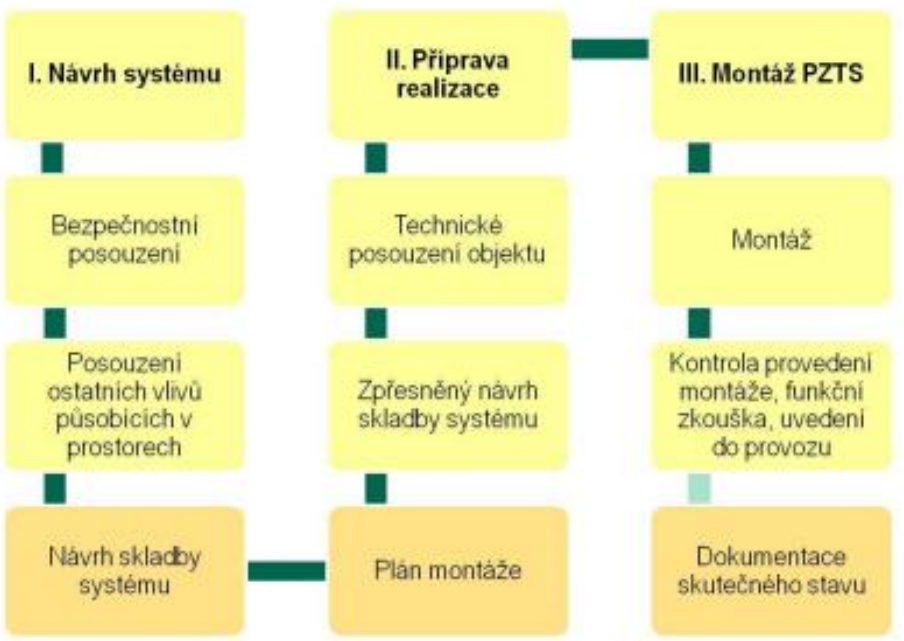
Na základě iniciační události, kterou je v tomto případě zloděj, který se snaží dostat do objektu a odcizit nám chráněné aktivum. Pomocí analýzy stromem událostí jsme schopni znázornit možné scénáře, jak si pachatel bude počínat.

4.2 Proces zřizování PZTS

Poplachové zabezpečovací a tísňové systémy jsou definovány jako kombinované systémy určené k detekci poplachu vniknutí a tísňového poplachu.

Činnosti spojené s procesem zřizování PZTS jsou:

1. Návrh systému
2. Příprava realizace
3. Montáž PZTS

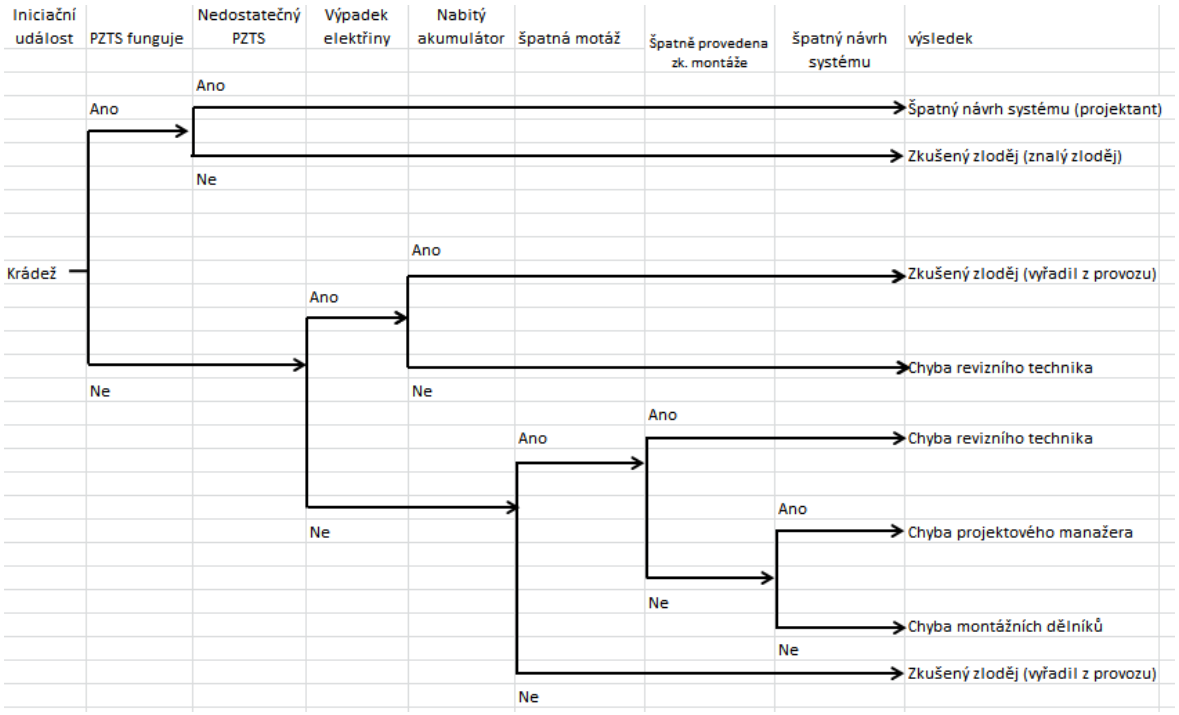


Obr. 19 Proces návrhu PZTS [10]

Výstupy ve formě dokumentů představují v jednotlivých etapách:

- Návrh skladby systému (systémový návrh, studie)
- Plán montáže (projektová dokumentace)
- Dokumentace skutečného stavu (dokumentace skutečného provedení stavby)

4.2.1 Použití analýzy stromem událostí pro proces zřizování PZTS



Obr. 20 Analýza stromem událostí pro proces PZTS, vlastní zdroj

Na obrázku je znázorněna jako iniciační událost krádež chráněného aktiva. Na základě toho pomocí analýzy stromem událostí zkoumáme, kde se stala v procesu chyba.

4.3 Proces převozu peněžní hotovosti a cenností

Jedná se o činnost, při které společnost přebírá na základě smluvního vztahu zodpovědnost za přepravu peněžní hotovosti a cenností. K realizaci této činnosti poskytne ozbrojený doprovod a potřebnou logistickou podporu. Proces se skládá z dílčích činností:

- Přípravná fáze přepravy peněžní hotovosti a cenností
  - Personální obsazení
  - Plánování přepravy
  - Výběr trasy
- Stanovení úloh a povinností přepravní skupiny
- Logistická příprava peněžní hotovosti a cenností
  - Přenos peněžní hotovosti a cenností
  - Přeprava peněžní hotovosti a cenností
- Taktika přepravy peněžní hotovosti a cenností

4.3.1 Kontrolní seznam pro přepravu peněžní hotovosti a cenin

		Přeprava peněžní hotovosti a cennin (přípravná fáze přepravy)	Ano	Ne
1		Proškolení pracovníci		
2		Dobrý zdravotní stav posádky		
3		Dostatečný počet ozbrojených pracovníků		
4		Rozdělení jednotlivých funkcí přepravy		
5		Seznam kontaktních osob		
6		Plánovací dokumentace:		
6	a	Půdorys okolí objektu včetně přilehlých ulic		
6	b	Vyzančení místa a způsob převzetí nebo předání cenností		
6	c	Směr výjezdu, příjezdu a parkování vozidla		
6	d	Trasu vozidla včetně náhradních tras		
6	e	Vyznačení veškerých rizikových míst, kterým se nedá operativně vyhnout		
6	f	Důležité telefonní čísla		
6	g	V případě použití více vozidel jejich rozmístění a úlohy		
7		Vykonání obhlídky trasy:		
7	a	Změna dopravního značení		
7	b	Přítomnost údržby silnic		
7	c	Spatření podezdřelých osob		

Obr. 21 Kontrolní seznam pro přepravu peněžní hotovosti, vlastní zdroj

Na základě připraveného kontrolního seznamu můžeme při přípravné fázi zjistit, zdali jsme na přepravu, náležitě vybaveni, máme záložní plán a další výše zmíněné věci. Kontrolní seznam se samozřejmě můžu s časem měnit a doplňovat a další poznatky, aby se předcházelo možným hrozbám.

ZÁVĚR

V práci jsou uvedeny teoretické základy managementu s bližším zaměřením na specifika bezpečnostního managementu. Na základě toho jsou v další kapitole popsány vlastnosti, které by měl schopný manažer ovládat.

Abychom pochopili, všechny aspekty a tributy procesu řízení rizik, je potřeba si nejprve definovat a vysvětlit jednotlivé termíny z této oblasti. Jsou zde uvedeny důležité definice, které jsou klíčové pro správné určení problému a jeho následného řešení.

Proces řízení rizik je velmi obsáhlý a skládá se z dílčích subprocesů, z kterých se věnuji zejména subprocesu posuzování rizik.

Ochrana majetku je v dnešní době, kdy jsou ve společnosti velké majetkové rozdíly, velmi důležitá pro ochranu našich aktiv. Proto jsem do této kapitoly uvedl základní druhy ochrany a pomocí jakých prvků je ochrana realizována.

Stěžejní část mé práce se věnuje analýzám rizik. Na začátku každé analýzy je zásadní otázka, jakým způsobem analýzu vytvářet. Od námi zvolené metody se odvíjí celý postup procesu, a proto je důležité si zvolit pro daný proces vhodnou metodu analýz rizik. V práci jsou uvedeny základní analýzy rizik, jejich popis a samozřejmě jejich klady a zápory.

V praktické části mé práce jsou uvedeny procesy v oblasti ochrany majetku a na některé z nich jsou aplikované analýzy rizik.

Analýzy rizik nám při vhodném a včasném použití pomáhá pochopit bližší podstatu jednotlivých problémů. Nemají téměř žádné omezení, dají se použít před začátkem procesu, na jeho začátku, v jeho průběhu a také po jeho ukončení. Výstupem analýzy rizik je seznam možných hrozeb a popsání jejich závažnosti.

SEZNAM POUŽITÉ LITERATURY

1. LUKÁŠ, Luděk, a kol. Bezpečnostní technologie, systémy a management II. Zlín: VeRBum, 2012. 384 s. ISBN 978-80-87500-19-4.
2. LUKÁŠ, Luděk, a kol. Bezpečnostní technologie, systémy a management III. Zlín: VeRBum, 2013. 456 s. ISBN 978-80-87500-035-4.
3. ŠAJDLEROVÁ, Ivana; KONEČNÝ, Milan. Základy managementu. Ostrava: Ediční středisko VŠB – TUO, 2007. 197 s. ISBN 978-80-248-1520-6.
4. HURTA, Josef; LAUCKÝ, Vladimír. Management bezpečnostního inženýrství. Zlín: Univerzita Tomáše Bati ve Zlíně, 2005. 172 s. ISBN 80-7318-412-5.
5. LAUCKÝ, Vladimír. Technologie komerční bezpečnosti I. Zlín: Univerzita Tomáš Bati ve Zlíně, 2009. 82 s. ISBN 978-80-7318-889-4.
6. ZEMAN, Petr. Česká bezpečnostní terminologie: výklad základní pojmů. Brno: Masarykova univerzita v Brně, 2003. 186 s. ISBN 80-210-3037-2.
7. ŠEFČÍK, Vladimír. Analýza rizik. Zlín: Univerzita Tomáše Bati ve Zlíně, 2009. 98 s. ISBN 978-80-7318-696-8
8. ČSN EN 31010, Management rizik. Zlín: Techniky posuzování rizik, Praha: Úřad pro technickou normalizaci, metrologii a zkušebnictví, 2011. 80s.
9. ČERMÁK, Miroslav. Řízení informačních rizik v praxi. Brno: Tribun EU, 2009. 134 s. ISBN 978-80-7399-731-1
10. VALOUCH, Jan. Projektování bezpečnostních systémů. Zlín: Univerzita Tomáše Bati ve Zlíně, 2012. 152 s. ISBN 978-80-7454-230-5.
11. Hulva, Tomáš. Ochrana majetku, Linde Praha, 2008. 376s. ISBN 978-80-7201-712-6

Internetové zdroje:

12. Vítězslav hálek [online] 2010 [cit. 2013-2-15]. Dostupné z: http://halek.info/www/
13. Odborné časopisy [online] 2006 [cit. 2013-3-08]. Dostupné z: http://www.odbornecasopisy.cz/vyznam-analyzy-metodou-hazop-pri-tvorbe-bezpecnostni-dokumentace-31467.html

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

BOZP Bezpečnost a ochrana zdraví při práci.

CCTV Closed – Circuit Television

EPS Elektronická požární signalizace

IZS Integrovaný záchranný systém

PZTS Poplachový zabezpečovací a tísňový systém

SEZNAM OBRÁZKŮ

SEZNAM TABULEK