NÁSTROJE PRO ZAJIŠTĚNÍ BEZPEČNÉ ORGANIZACE

TOOLS FOR SAFE ORGANISATION ENSURING

Dana PROCHÁZKOVÁ
prochazkova.dana@ujak.cz

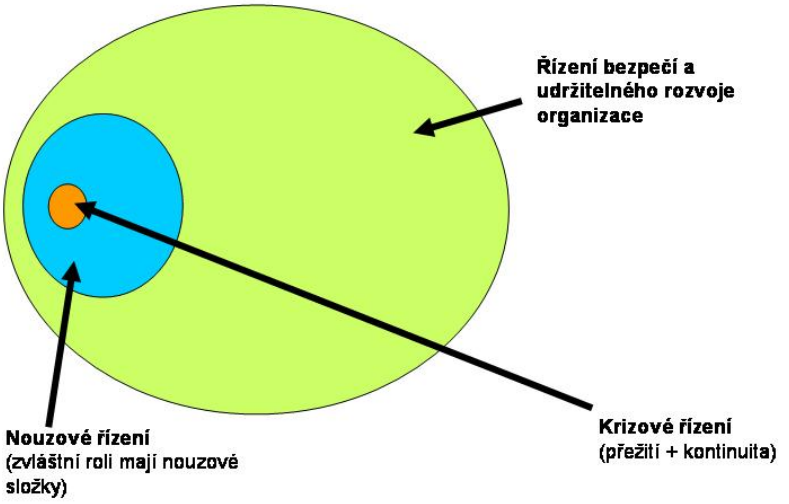
Abstract

To ensure the safe organisation with a potential do develop sustainable there is necessary: to know and to consider all possible risks inside and outside of organisation, namely in details and contexts; to negotiate with risks correctly; to apply correctly adjusted risk management; and to use qualified tools for risk management profiting the security. With regard to present knowledge there is necessary to consider the organisation as an open system the behaviour and state of which have been affected by processes and phenomena being under way inside and outside of system. Their impacts have been modified by complicated networks of links and flows that are inside of partial systems, across partial systems, across the whole system and in organisation surrounding. The risk management must be, therefore, complex and its priorities must be directed to the organisation security and its sustainable development. Because the sources, forces and means of each organisation are limited and its disposal has been also depending on conditions being in organisation surrounding, the organisation governance must competently handle with them in order that required aims might be reached.

Key words
Good Governance. Risk Determination. Risk Management. Safety Management. Planning for Security. Safety Management System.

1. Úvod do problematiky

V právním státě každá organizace musí kromě cílů, ke kterým byla zřízena, respektovat cíle státu, morální a etická pravidla lidské společnosti v místě, ve kterém působí. Z hlediska základní funkce státu to znamená, že chráněné zájmy státu reprezentují veřejný zájem a jsou předřazené vlastním chráněným zájmům organizace. Správné řízení věcí ve prospěch veřejného zájmu i zájmu organizace má na základě současného poznání formu projektového a procesního řízení organizace, které je upravené provázaným souborem opatření a činností a ve kterém hlavní roli hraje vyjednávání s riziky [1,2]. Správné řízení věcí má tři úrovně (obrázek 1), a to:



Obr. 1
Úrovně správného řízení věcí v organizaci chápané jako systém

- cílené řízení bezpečnosti, ve kterém jde o bezpečí a udržitelný rozvoj organizace chápané jako systém, tj. jde o zajištění bezpečí a udržitelného rozvoje chráněných zájmů sledované organizace. Hlavní zacílení řízení je lidské činnosti a lidmi aplikovaná opatření provádět tak, aby změny ve sledované organizaci vyvolané výskytem škodlivých jevů (označených dále slovem pohromy) se zdrojem uvnitř i vně organizace nevedly k nepřijatelnému narušení až zániku organizace, tj. aby lidmi aplikované činnosti a opatření vedly k zabránění výskytu možných pohrom a nebo alespoň ke zmírnění jejich škodlivých dopadů na organizaci,
- nouzové řízení, které se používá v případech, ve kterých se vyskytly závažné problémy a je třeba provést činnosti a opatření, aby ztráty, škody a újmy na chráněných zájmech organizace byly přijatelné s tím, že se používají standardní zdroje, síly a prostředky organizace,
- krizové řízení, které se používá v případech, ve kterých se v organizaci vyskytly kritické problémy a je třeba provést činnosti a opatření, aby ztráty, škody a újmy na chráněných zájmech organizace uvnitř i vně byly přijatelné s tím, že se používají standardní i nadstandardní zdroje, síly a prostředky organizace i spolupráce s veřejnou správou a dalšími organizacemi, které jsou v místě nebo jsou profesně příbuzné. Hlavní pozornost je věnována životům a zdraví lidí a životnímu prostředí a zajištění přežití organizace.

Správné řízení věcí v organizaci není možné bez znalosti rizik a jejich efektivního řízení. Z globálního pohledu jsou rizika, kterým musí každá organizace čelit, spojená s:

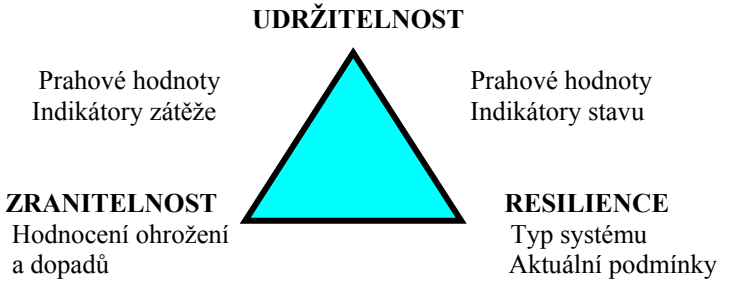
- pohromami, tj. škodlivými jevy, jejichž původ je uvnitř i vně organizace,
- dopady pohrom,
- zranitelnostmi organizace, jejich chráněných zájmů a jejího okolí,
- domino efekty, které se mohou vyskytnout v organizaci nebo jejím okolí,
- vnitřními vazbami v organizaci,
- lidským faktorem,
- chybami při řízení a správě organizace, a to hlavně při opatřeních a činnostech odezvy a obnovy, které jsou obvykle prováděné v časovém presu,
- náhodnými kombinacemi možných jevů, které mohou v organizaci vzniknout.

Řízení či správa věcí organizace je založena na kvalifikovaném plánování a systémově propojuje všechny životně důležité sektory pro zajištění bezpečí a udržitelného rozvoje organizace [2]. Toto poznání platí jak pro veřejný, tak pro privátní sektor, ve kterém do věcí spojených s bezpečím a udržitelným rozvojem přibývá ještě zajištění zisku, který je zdrojem obživy i dalších investic, a proto do souboru rizik přibývají také specifická rizika jako: riziko ztráty zisku; a riziko ztráty souladu s požadavky veřejné správy v daném území.

V současně upřednostňovaném pojetí se předpokládá, že bezpečí má i rozměr budoucí, tj. nestačí zajistit jen současný žádoucí stav systému, kterým je každá organizace, ale i jeho žádoucí stav v budoucnosti blízké a pokud možno i vzdálené, tj. bezpečí zahrnuje v sobě takový rozvoj systému, ve kterém je zaručeno bezpečí i v budoucnosti, tj. jde o udržitelný rozvoj (tj. rozvoj podporující rozvoj člověka i lidské společnosti žádoucím směrem v čase) [2,4-9]. Je si třeba uvědomit, že ve všech úvahách o bezpečí a udržitelném rozvoji je nutno zvažovat i okolí systému, protože každá organizace je otevřený systém.

Udržitelnost / udržitelný rozvoj každého systému je z odborného hlediska koncept, který je ukotven v čase a vztahuje se k systému jako celku. Podle práce [9] platí, že pro podporu bezpečné organizace je třeba udržitelný rozpočet organizace. Tento způsob hledání rovnováhy odráží fakt, že současný ekonomický růst nemá zabudovány mechanizmy pro dlouhodobé přežití (speciálně nemá dostatečnou houževnatost - resilience).

Ze systémového hlediska organizace vytvářená jako udržitelný systém musí mít atributy ***produktivity, resilience,*** (houževnatosti = stabilita a spolehlivost), ***adaptability*** a ***zranitelnosti.*** To znamená, že tři základní atributy jsou odlišné, ale i vzájemně provázané, souvislosti ukazuje obrázek 2, na kterém jsou ještě vyznačené faktory, které identifikují atributy a jejich souvislosti. Protože sledované vlastnosti jsou vzájemně spjaty, tak ve vztahu k existenci systému je na vrcholu udržitelnost. Rozhodování o adaptivní kapacitě systému je pak dáno vztahem, který je uveden v rozhodovací matici v tabulce 1.



Obr. 2
Vztah mezi udržitelností, zranitelností a houževnatostí (resilience)

Cílem řízení udržitelnosti organizace prostřednictvím řízení rizik nebo vyššího typu řízení, tj. prostřednictvím řízení bezpečnosti, je zabránit, aby se systém nedostal do nežádoucích, tj. nepřijatelných stavů a uspořádání [10]. Řízení udržitelnosti musí vycházet z řízení resilience [11], které má dva cíle:

1. Zabránit, aby se systém dostával do nežádoucích stavů v důsledků vnějších poruch a vnější zátěže.
2. Uchovat prvky aktivující systémovou reorganizaci a obnovu v důsledku masivních změn.

Tabulka 1
Adaptivní kapacita systému

Dopady	**Adaptivní kapacita**	
	Nízká	***Vysoká***
Vysoké	*Zranitelnost*	Příležitosti rozvoje
Nízké	Zbytková rizika	*Udržitelnost*

Z hlediska řízení rizik [2] je nutné také věnovat péči snižování zranitelnosti systému a posilování adaptability systému, protože ***udržitelnost je neustálé přizpůsobování systému měnícím se podmínkám*** [10]. Proto je žádoucí používat a rozpracovat metodiku předvídavosti nejen na technologické, ale i na společenské úrovni (societal foresight), která se zaměřuje na trendy chování lidmi vytvořeného prostředí (např. teorie normálnosti havárie, vysoce spolehlivé organizace, industriální ekologie) a životního prostředí (např. teorie adaptivního environmentálního managementu, industriální ekologie apod.).

Z výše uvedeného vyplývá, že cílem různých analýz by nemělo být jen výčtové stanovení kritických prvků, kritických jevů apod., ale cílem by mělo být monitorování udržitelné existence (sustainable livelihoods), protože v ní se kumulují všechny vlivy udržitelné organizace a jejího okolí. V práci [12] se uvádí,

že metody vhodné pro analýzu udržitelnosti existence (bytí) musí specifikovat parametry pro různou systémovou udržitelnost, tj. pro udržitelný:

- ekonomický a technologický systém, tj. pro rozmanitost odvětví, kvalifikovanou pracovní sílu, inovace, robustní infrastruktury, účelný pohyb zboží a služeb, dostupnost technologií, eko-účinnost,
- sociální systém, tj. pro soudržnost komunity, sociální kapitál, ochranu, bezpečnost a bezpečné prostředí, vztah k místu, udržování kulturního dědictví, mobilitu, rovnost příležitostí, zelenou infrastrukturu a rekreační možnosti,
- environmentální systém, tj. pro zdravou a kvalitní půdu, biorozmanitost, funkční zelenou infrastrukturu, biokoridory a propojené biolokality, environmentální toky, kvalitu vody a ovzduší, charakter krajiny.

Zajištění udržitelnosti těchto systémů vyžaduje kvalitní správu, tj. transparentnost a odpovědnost v rozhodování, kompetentnost, schopnost předjímat budoucí situace.

2. Soubor poznatků pro řízení rizik

Bezpečí a udržitelný rozvoj organizace závisí na tom, jak se vypořádáváme s riziky, tj. v prvé řadě na tom, zda rizika v organizaci existující v době současné i předvídatelná rizika v době budoucí správně vyhledáme, pochopíme a vyhodnotíme a zda s nimi optimálně naložíme. Vyjednávání s riziky spočívá v tom, že správně musíme ocenit velikost možných pohrom všeho druhu, které jsou zdrojem rizik pro organizaci. Pohromy mají zdroje jak uvnitř, tak vně organizace.

V řízení zaměřeném na rizika odlišujeme dva základní pojmy, a to ohrožení a riziko. ***Ohrožení***, anglicky *hazard*, je velikost konkrétní pohromy určená podle stanovených pravidel, která působí na danou organizaci. ***Riziko***, anglicky *risk*, je pravděpodobná velikost nežádoucích dopadů (ztrát, škod a újmy) způsobených pohromou o velikosti ohrožení na chráněné zájmy v dané organizaci určená podle stanovených pravidel. Závisí jednak na velikosti ohrožení pro danou organizaci a jednak na zranitelnosti organizace vůči konkrétní pohromě, a to územní (náchylnost ke ztekucení, propadnutí, sesuvu), technické (náchylnost ke vzniku domino efektu), určené počtem lidí a jejich rysy [13] nebo finanční (nedostatek použitelných finančních prostředků), znalostní (nedostatek kvalifikovaného personálu) atd.

Rizika stále přibývají a lidská společnost nemá zdroje, síly a prostředky, aby tomu zabránila, tak musí cíleně řídit rizika. Aby řízení bylo úspěšné, tak se musí zaměřit na prioritní rizika a jejich aspekty. Prioritní rizika jsou taková rizika, při jejichž realizaci průměrné škody, ztráty a újmy na chráněných zájmech vztažené na zvolenou časovou jednotku (např. 1 rok) jsou větší než zvolená hranice přijatelnosti.

Vyjednávání s riziky [14] vychází ze současných možností lidské společnosti a spočívá v rozdělení vypořádání rizik do kategorií, ve kterých se příslušná část rizika zajistí tak, že se:

- sníží , tj. preventivními opatřeními se odvrátí realizace rizika,
- zmírní, tj. účelovými preventivními opatřeními odezvy a připraveností (varovné systémy a jiná opatření nouzového a krizového řízení) se sníží nebo odvrátí nepřijatelné dopady při realizaci rizika,
- pojistí,
- připraví rezervy na odezvu a obnovu a zálohy pro zajištění přežití lidí a kontinuitu provozu organizace,
- připraví plán pro odezvu na nepředvídané situace (contingency plan) v případě rizik neřiditelných nebo příliš nákladných na eliminaci a nebo málo častých.

K tomu se rovněž připojuje rozdělení zvládání rizik mezi všechny zúčastněné. Rozdělení ve správném řízení se provádí tak, že se vychází z toho, že za zvládání rizik odpovídají všichni zúčastnění a že zvládání konkrétního rizika je nejlépe přidělit tomu subjektu, který je na to nejlépe připraven [1]. Toto je však možné jen v organizaci, ve které je kvalifikované projektové a procesní řízení, tj. činnosti a opatření se aplikují na základě znalostí, a to věcných i z oblasti řízení (tj. činnosti jsou vzájemně provázané, nejsou chyby v komunikaci, každý zúčastněný ví, co má dělat a jak to má dělat).

3. Stanovení rizika

Analýza a hodnocení rizik v organizaci se provádí tak, že se systematickým postupem zjistí dopady pohrom, které se mohou vyskytnout v organizaci nebo v jejím okolí a ovlivnit organizaci nežádoucím způsobem (tj. v úvahu se berou jen relevantní pohromy a z důvodu omezenosti zdrojů všeho druhu především pohromy, které pro organizaci patří mezi specifické a kritické pohromy [7]. Pro každou pohromu se vytvoří procesní model, který znázorňuje její působení na prvky, vazby a toky organizace, která je chápaná jako systém, tj. zvažují se nejen přímé dopady pohromy na chráněné zájmy organizace, ale i dopady pohromy zprostředkované složitou sítí vazeb a toků v organizaci a jejím okolí s tím, že zvláštní pozornost je věnována chráněným zájmům. Poté se pro stanovenou velikost pohromy vypočtou škody, ztráty a ujmy na chráněných zájmech a stanoví se riziko ***způsobem, který je správný, transparentní a opakovatelný***.

Z metodického hlediska známe riziko integrální, integrované a dílčí:

- dílčí riziko je riziko vztažené k jednomu chráněnému zájmu. Postupy pro jeho stanovení jsou dané směrnicemi, právními předpisy, normami, standardy a tzv. dobrou praxí,
- integrální a integrované riziko uvažuje soubor chráněných zájmů. Integrální riziko se zjišťuje se systémovým přístupem, postupy jsou dané směrnicemi, právními předpisy, normami, standardy. Integrované riziko je součet

(aritmetický, vážený aj.) dílčích rizik pro všechny zvažované chráněné zájmy. Postupy pro jeho stanovení jsou dané směrnicemi, právními předpisy, normami, standardy. Integrované riziko často používají pojišťovny.

Z výše uvedených skutečností vyplývá, že pro stanovení rizik organizace je důležité:

- jaké jsou chráněné zájmy organizace (zde si je třeba opět uvědomit, že do nich patří jak chráněné zájmy státu, které jsou vynucovány právními předpisy či etickými a morálními pravidly v prostředí, ve kterém se organizace nachází, tak vlastní chráněné zájmy organizace, které jsou nutné pro existenci a rozvoj organizace),
- které jevy vnější i vnitřní působí v dané organizaci dopady na chráněné zájmy, které nejsou přijatelné (tj. představují pohromy),
- jak probíhají procesy, jejichž výsledkem je realizace rizika,
- vůči jaké velikosti pohromy (k jejímu označení se používá pojem projektová pohroma) je organizace odolná, tj. pohroma působí v organizaci jen dopady, které jsou přijatelné nebo podmíněně přijatelné, tj. organizace je ve všech směrech připravená uvedené dopady zvládnout,
- jak často se vyskytuje nadprojektová pohroma a co v organizaci působí a zda má organizace nějaká opatření vůči nadprojektovým pohromám, např. plán kontinuity [2],
- které dopady pohrom jsou nepřijatelné a mohou vést k rozkladu až zániku organizace.

Pro vybrané modely procesů existují konkrétní metody pro stanovení rizik, z nichž některé mají i softwarovou podporu [3]. Je si však třeba uvědomit, že i modely stejných procesů jsou zaměřené na určité cíle a jsou buď jednoduché, nebo složitější. Proto při výběru z existujících metod je třeba respektovat požadavky transferu technologií a ověřit, zda metoda je pro daný případ a cíl použitelná, či ne [2]. Obecně povaha metod je kvantitativní, kvalitativní i semikvantitativní. Podle cíle je nutno odlišovat metody, které jsou vhodné pro:

1. Identifikaci rizika.
2. Stanovení hodnoty rizika, ve kterém jde o přesný údaj pro potřeby strategického rozhodování.
3. Stanovení hodnoty rizika pro potřeby kontroly rizika konkrétního procesu v čase a prostoru, při kterém lze použít míru (a to i verbální) a o taktické a operativní rozhodování.

Aby řízení / správa organizace mohla pracovat účinně s riziky, je třeba stanovit postup pro stanovení rizik právním předpisem a zároveň je třeba stanovit hodnotové stupnice, dle kterých se interpretují výstupy z nástrojů na stanovení rizik v organizaci, tj. je třeba určit, co je přijatelné, co je podmíněně přijatelné a co je nepřijatelné. Mezi nástroji pro stanovení rizik je třeba odlišit sofistikované nástroje pro odbornou sféru a nástroje pro řízení / správu organizace, pro kterou jsou nejvhodnější kontrolní seznamy [2].

Riziko pro správné strategické rozhodování a strategické řízení se stanovuje jedním z dále uvedených přístupů [14]:

1. Určení ohrožení organizace od konkrétní pohromy H a periody návratu τ (v rocích). Z nich se na základě možných dopadů určí S = celková škoda pro ohrožení H v dané organizaci (nejlépe v penězích). Riziko R vztažené ke zvolené časové jednotce se spočte dle vztahu

$$R = \frac{S}{\tau} .$$

2. Určení scénáře pohromy o velikosti největší očekávané pohromy a podle něho:
   a) podle chráněných zájmů organizace a jejich zranitelnosti vůči dopadům ve scénáři pohromy se určí hodnota S = celková škoda v dané organizaci (nejlépe v penězích),
   b) podle odborných údajů určujících maximální možnou velikost pohromy nebo expertních odhadů na základě databází se určí četnost výskytu největší očekávané pohromy normovaná na 1 rok f. Tento postup je obvyklý u rizik spojených s množstvím nebezpečných látek v průmyslových objektech.

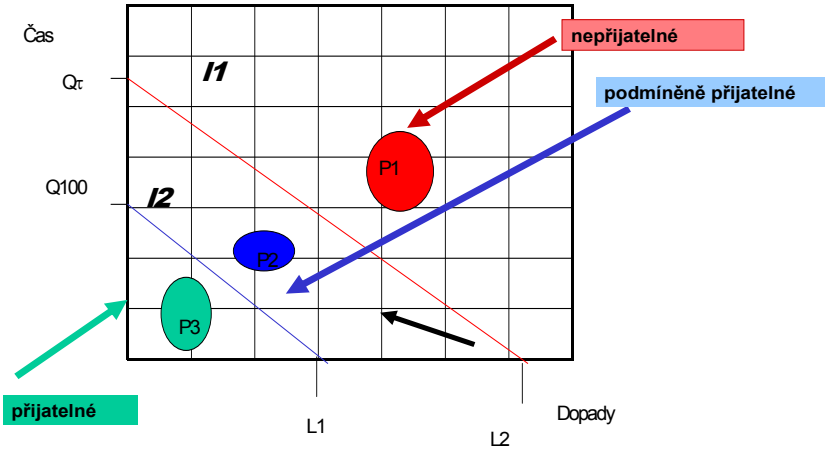
   Riziko R vztažené ke zvolené časové jednotce se spočte dle vztahu

$$R = S * f .$$

Po stanovení velikosti rizika následuje hodnocení přijatelnosti rizika, což je strukturovaná procedura, která se pokouší odpovědět na dále uvedené otázky:

- jaké ztráty, škody a újmy budou na chráněných zájmech organizace?
- jak často se ztráty, škody a ujmy stanou?
- jak zareagují bezpečnostní systémy v organizaci a jejím okolí?
- jaké ztráty, škody a újmy budou na chráněných zájmech organizace, když selžou bezpečnostní systémy v organizaci nebo v okolí organizace?

Po vyhodnocení odpovědí na výše uvedené otázky se určí způsob vyjednávání s jednotlivými zjištěnými riziky [2]. Obvykle se rozhoduje na základě rozhodovací matice [2,7]. Příklad podkladu pro rozhodování je na obrázku 3.



Obr. 3
Perioda výskytu pohromy vs. velikost dopadů pohromy
Q100 = 100 let, Qτ = střední perioda opakování pohromy o normativní velikosti,
L1 = výše pojištění, L2 = desetina ročního rozpočtu organizace.

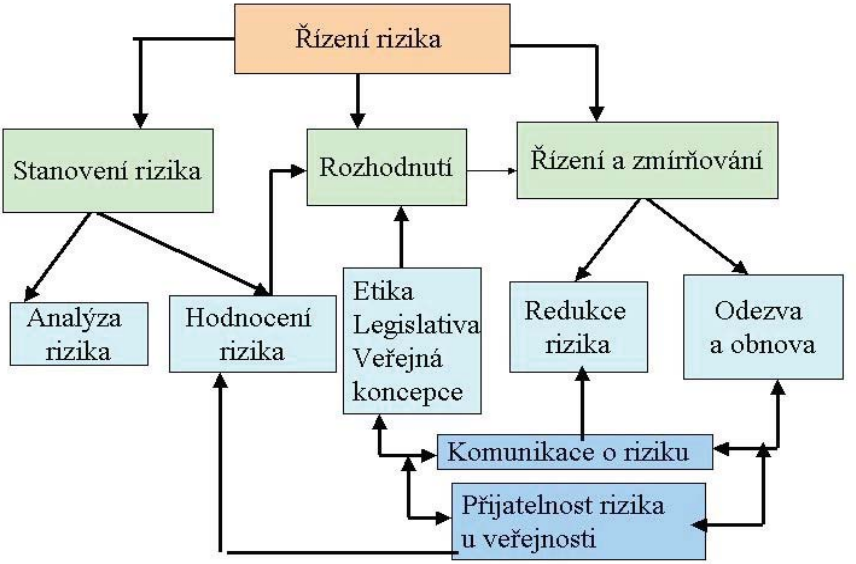
4. Modely řízení rizika

Každodenní fakta i analýzy chování lidského systému ukazují, že rizika jsou existující realitou a že v čase se objevují stále nová rizika. Proto je třeba žít podle koncepce život s riziky. Tato koncepce upravuje postup správy organizace následovně:

- definice chráněných zájmů organizace (včetně těch, které musí organizace ctít dle pravidel daných veřejnou správou),
- stanovení cílů na úseku bezpečí a rozvoje chráněných zájmů,
- zajištění cílů pomocí opatření a činností prevence, připravenosti, odezvy a obnovy.

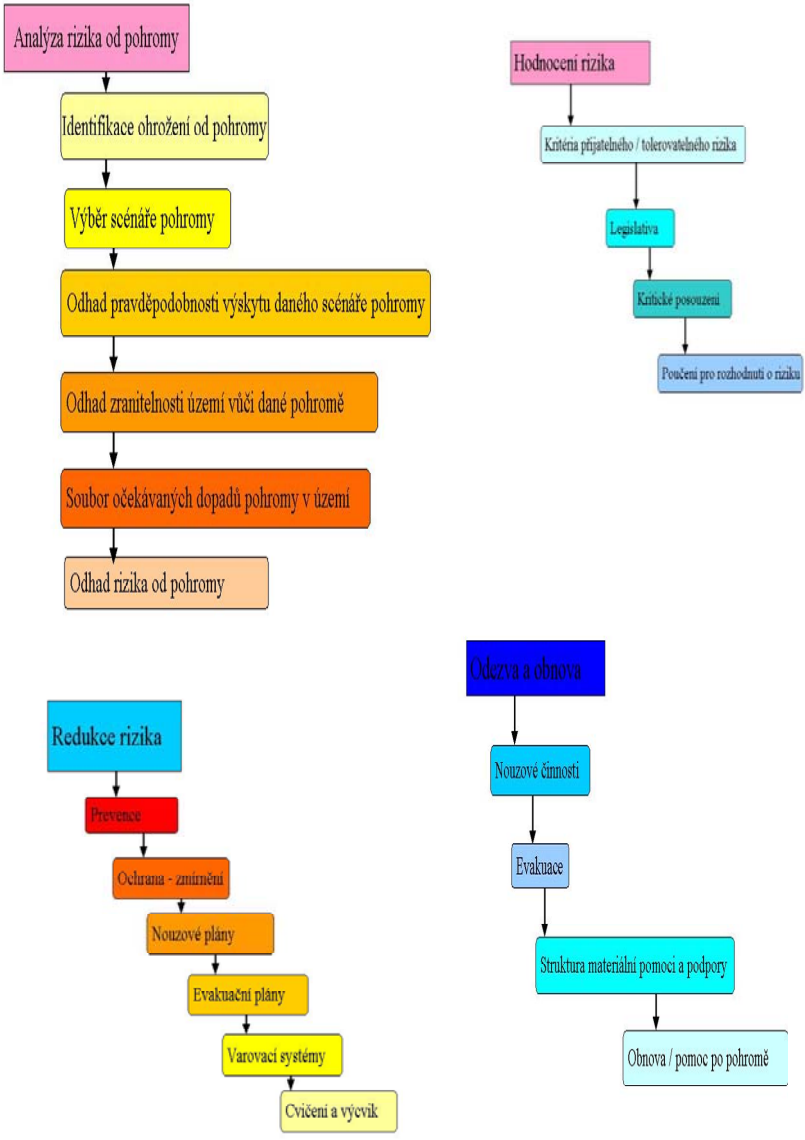
Dle klasického modelu řízení rizika [2,7] (obrázky 4 a 5) se řízení rizika v organizaci provádí tak, že se zvažují rizika od jednotlivých pohrom odděleně a pozornost se věnuje jen rizikům, jejichž pravděpodobnost výskytu je větší než určitá hodnota (obvykle 0.05). Každá pohroma se řídí odděleně a systémově se nekontroluje, zda opatření provedená ke snížení rizika od jedné pohromy nevedou ke zvýšení rizika od jiné možné pohromy, která postihne organizaci. Obrázek 4 ukazuje pořadí operací, které musí být provedeny k tomu, aby rizika byla správně řízená. Obrázek 5 pak ukazuje základní kroky pro dílčí operace, které

musí být provedeny k tomu, aby rizika byla správně řízená. Oproti tradičním postupům v technických normách jsou na obrázku 4 vyznačeny i otázky komunikace o riziku a jeho přijatelnosti, a to dle postupů přijatých EU a zapracovaných v české legislativě do zákonů o EIA.



Obr. 4
Model klasického řízení rizika [2,7]

Řízení bezpečnosti, tj. řízení rizik ve prospěch bezpečí v organizaci [2,7], obrázek 6, se provádí tak, že se zvažují všechna rizika od všech možných pohrom v dané organizaci ***DOHROMADY*** a dle stanovené úrovně bezpečnosti se vybírá soubor optimálních opatření pro vyjednávání se všemi specifickými a kritickými pohromami (dle [3] relevantní pohroma je taková pohroma, která působí na organizaci, ale její dopady jsou přijatelné; specifická pohroma je pohroma, která má na organizaci nepřijatelné dopady; kritická pohroma je taková pohroma, která má kritické dopady, které mohou vést k rozložení až zániku organizace). Pozornost se věnuje i rizikům, která jsou málo pravděpodobná, ale dopady s nimi spojené vyvolají nebo mohou vyvolat velké ztráty, škody a újmy na chráněných zájmech, tj. uplatňuje se ***PRINCIP PŘEDBĚŽNÉ OPATRNOSTI***. Obrázek 6 ukazuje, že rozhodujícím faktorem, který hraje roli v řízení bezpečnosti nejsou jednotlivá integrální rizika pohrom, ale zbytkové integrální riziko určené pro všechny relevantní pohromy v konkrétní entitě (místě / organizaci). Obrázek též ukazuje umístění monitoringu v procesu řízení bezpečnosti.

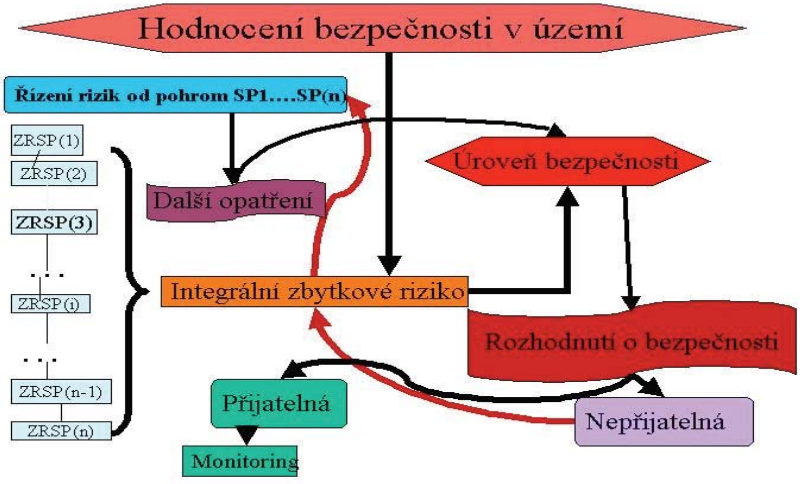


Obr. 5
Specifikace základních kroků klasického řízení rizika [2,7]

Přechod od klasického řízení rizik na řízení rizik znamenající vypořádání rizik ve prospěch bezpečí a udržitelného rozvoje (anglicky Risk Governance) [2,7] v praxi znamená:

- stanovit synergické vztahy mezi riziky, zranitelností a bezpečím,
- modelovat proces rozhodování správy organizace s ohledem na rizika, nejistoty a neurčitosti (viz podpůrné systémy rozhodování),
- specifikovat rámcové právní podmínky a ochranná opatření,
- zlepšovat činnosti institucí (institucionální změny).

Problematika řízení rizik je zásadní a vyžaduje odborný postup [1-3,7,13,14].



Obr. 6

Model řízení rizika ve prospěch bezpečí a udržitelného rozvoje [2,7]

Pro klasické řízení rizik i pro řízení rizik ve prospěch bezpečí, tj. řízení bezpečnosti [2], je nutné:

1. Rozumět procesu vzniku pohrom a podmínkám, ve kterých proces probíhá.
2. Znát, ve kterých místech pohroma může vzniknout a jaké může mít fyzikální a jiné charakteristiky.
3. Identifikovat ohrožení, které představuje v daném místě pohroma dle stanovených standardů.
4. Stanovit dopady projektových pohrom (tj. normativních ohrožení) na chráněné zájmy.
5. Eliminovat nepřijatelné dopady pohrom v případech, ve kterých to jde za přijatelných nákladů.

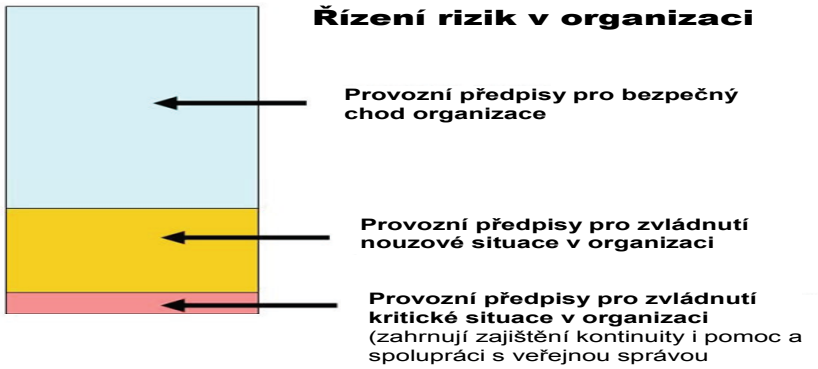
6. U zbylých dopadů vypočítat pomocí prognostických modelů pravděpodobnost jejich realizace s tím, že se vezmou v úvahu i možná selhání preventivních opatření.
7. Vypočítat možné škody na chráněné zájmy v konkrétní organizaci a jejím okolí podle chráněných zájmů, které jsou skutečně v organizaci a jejím okolí a na základě pravděpodobností určit výši rizika.
8. Identifikovat a realizovat zmírňující opatření s ohledem na lidi, majetek a životní prostředí tak, aby byla ALARP (tak malá, jak je rozumně možné dosáhnout).
9. Prokázat, že byla provedena všechna opatření k zabránění a zmírnění dopadů pohrom.

Přijatelné riziko lze dosáhnout snížením ohrožení od konkrétních pohrom, což však jde jen u pohrom, které souvisí s činností člověka, a dělá se to snížením zranitelnosti organizace, která je předmětem hodnocení rizika [2]. Mechanismus zvládání rizik v organizaci je znázorněn na obrázku 7. Uvedený obrázek ukazuje, že provozní předpisy i legislativní předpisy z pohledu zajištění bezpečnosti subjektu vůči předmětné pohromě mají po odborné stránce jednotnou strukturu, tj. provázané soubory opatření pro zajištění bezpečí a rozvoje, opatření při nouzové situaci a opatření při kritických situacích. Ukazuje také, ve kterých místech stát posiluje úsilí o zajištění bezpečnosti a zajišťuje připojení specializovaných výkonných složek, které pomáhají stabilizovat situaci a ochraňovat chráněné zájmy s cílem, aby ztráty, škody a ujmy byly přijatelné.

5. Aspekty důležité pro řízení rizika uvnitř organizace

Organizace je z odborného pohledu systém systémů. Problémy z hlediska současného poznání jsou:

1. Popis a charakteristika systému, který má více chráněných zájmů chápaných systémově, a mezi nimi existují různé vnitřní vazby a toky.
2. Odolnost, zranitelnost a adaptabilita jednotlivých systémů i systému systémů. Kdy (při jaké kombinaci vlastností) je systém udržitelný?
3. Určení integrálního rizika (v systému je více chráněných zájmů, které jsou propojené vnitřními vazbami) pro zdroje rizik uvnitř i vně systému.
4. Vztahy mezi dílčím, integrovaným a integrálním rizikem systému.
5. Vztahy mezi integrálním rizikem systému a integrálními riziky podsystémů.
6. Kritéria pro integrální bezpečnost systému systémů (soubor bezpečných systémů nemusí být bezpečný – existují interdependences).
7. Zásady pro řízení bezpečnosti systému systémů (nutné např. pro kritickou infrastrukturu).
8. Legislativa pro podporu řízení bezpečnosti systému systémů.
9. Kontrolní mechanismy pro monitorování (úrovně) bezpečnosti systému systémů.



Obr. 7
Nástroje pro zvládání rizik v organizaci

6. Plánování pro podporu řízení rizika v organizaci

S ohledem na současné poznání je třeba sledovat v organizaci vnitřní závislosti, které zprostředkovávají sekundární a další dopady pohrom na chráněné zájmy organizace. K tomuto cíli je třeba:

- zavést do praxe monitoring bezpečnosti,
- dopracovat a kodifikovat metodiky pro sběr dat, odborné zpracování veličin nutných pro rizikovou analýzu v systému systémů,
- vypracovat metodiky pro rozhodování o rizicích a provázané systémy kontrolních seznamů na podporu rozhodování,
- pro zaměstnance vypracovat soubory opatření o tom, co mají dělat před, při a po pohromě, která v organizaci patří mezi specifické či dokonce kritické pohromy,
- pro potřeby strategického řízení organizace zpracovat plány pro zajišťování bezpečí a rozvoje organizace, nouzové plány, plány kontinuity a krizové plány organizace, které budou navzájem provázané a ve kterých jsou podchyceny úkoly řízení bezpečnosti a rozvoje za všech okolností,
- zajistit podpůrné systémy pro podporu řízení bezpečnosti, protože kvalifikovaná řešení vždy ušetří peníze, síly i prostředky. Dosavadní poznání totiž ukazuje, že zjednodušená řešení jsou možná jen někdy, ale i v případech, ve kterých jsou možná, je třeba znát, jaká zjednodušení situace byla provedena, proč je bylo možno použít a zda není třeba po nějaké době provést opatření další.

Nástroje bezpečnostní politiky, kterou se řízení bezpečnosti uvádí do praxe, jsou:

- koncepce, které vytyčují cíle bezpečnostní politiky,

- strategie, které určují základní způsoby, kterými bude cílů dosaženo,
- plány, které podrobně popisují a zahrnují činnosti v určitém časovém harmonogramu,
- nástroje a instituce, tj. zdroje, síly a prostředky, kterými se dosahuje splnění cílů bezpečnostní politiky.

Plánování je vědomé usměrňování rozvoje ke zvolenému cíli. Je to uvědomělá činnost řídících subjektů, která spočívá ve volbě a předpokládání cílů, úkolů, variant a způsobů, které podmiňují dosažení těchto cílů. Za nejdůležitější rys plánování se považuje volba cíle. Plánování není sestavení hierarchického souboru příkazů, které se mají bezmyšlenkovitě plnit, je to tvůrčí činnost, která má stanovit reálný cíl a určit nejvýhodnější způsob jeho dosažení. V praxi se setkáváme s mnoha druhy plánování, např. roční, oblastní, perspektivní, územní, vstřícné aj.

Plánování tvoří základní úsek každého řízení. Proto musí specifikovat nejen cíle, ale i možné varianty dosažení žádoucích cílů řízení, provést jejich vyhodnocení a výběr optimální varianty s ohledem na disponibilní síly, prostředky a zdroje. Poté je třeba provádět monitorování úspěšnosti vybrané varianty s ohledem na žádoucí cíl a systematicky odstraňovat nesoulady a překážky na cestě k realizaci vybraného cíle a přitom zabránit deformacím a ztrátě iniciativy účastníků procesu. K dosažení dlouhodobých cílů se používá strategické plánování a pro dosažení krátkodobých cílů plánování operativní; obě mají svá specifika, které předurčují výběr metod a způsobů.

Pro podporu správného řízení organizace je také nutné analyzovat každou nouzovou situaci a přijmout poučení, tj. podklady pro zlepšení prevence, zajištění zmírnění dopadů příští situace na chráněné zájmy, pro zlepšení odezvy atd. Z výsledků prezentovaných na konferenci TIEMS (Praha, červen 2008) [15] vyplynulo:

a) Při každé větší nouzové situaci je třeba v rámci poučení:
   - určovat slabé a silné stránky organizace a jejího systému řízení,
   - získat poznatky pro zvýšení odolnosti organizace s tím, že bude zvyšována adaptabilita,
   - získat poznatky pro to, abychom robustní systémy odezvy zaměřovali správně.
b) Pro podporu řízení nouzových situací nestačí jen jednooboroví specialisté, ale je třeba mít specialisty, kteří znají více oborové a mnohaoborové disciplíny a systém řízení organizace v daném případě. Každá organizace si musí tento odborný potenciál vybudovat k tomu, aby byla schopna zvládat rozsáhlé nouzové a kritické situace.
c) Tým pro řízení nouzových situací se musí skládat z vysoce zkušených lidí, musí mít určitou nezávislost při rozhodování a musí mít vlastní zdroje pro činnosti odezvy. Jeho úkolem je zajistit urgentní a bezprostřední odezvu, řešit neočekávané problémy, orientovat se na důsledky, zajistit kvalifikovanou odezvu za přijatelných zdrojů, sil a prostředků.
d) Je nutné zvyšovat neustále bezpečnost organizace i procesů, jichž se účastní zaměstnanci.

e) Odezva na hurikán Katrina v USA ukázala jeden důležitý fakt - za hranicemi kompetencí se v kritické situaci nedá téměř nic pořádného udělat. Proto je důležité pro zvládnutí všech situací mít předem připravené rozdělení kompetencí pro všechny možné situace, tj. i pro ty téměř nemožné.
f) Zkušenosti získané studiem odezev na nouzové situace velkého rozsahu ukázaly, že práce, které se dělají v rámci odezvy na kritickou situaci musí být:
   - jasné,
   - snadno proveditelné,
   - rychlé, aby podpořily účinnost akcí,
   - vést k výsledku.

Základní druhy plánování, které podporují základní úrovně řízení jsou bezpečnostní plánování, nouzové plánování a krizové plánování. V české praxi není ani bezpečnostní plánování, ani nouzové plánování sjednoceno pod agregovaný název a v jednotlivých oblastech a sektorech se používají dílčí názvy.
Pro plánování chápané jako činnost, kterou se vytváří podklady pro rozhodování v budoucích situacích je důležitý popis situace a představa o možných změnách (zjišťování míry nebezpečí pro určité časové období a určitou lokalitu). Proto se skládá ze dvou činností:

- ***předvídání*** možných situací a změn,
- jejich ***monitorování*** a ***programování*** reakcí na změny.

Provedené teoretické analýzy i rozbory praktických postupů [15] ukázaly na nutnost při plánování obecně dodržovat určité zásady jako:

1. Plánovat s nadhledem, tj. neplánovat pro případy konkrétních pohrom, protože při výskytu konkrétních jevů jsou různé podmínky a dochází ke kumulaci různých faktorů, které zesilují nebo zeslabují působení pohromy a mění situaci v organizaci.
2. Nouzové situace vyvolané pohromami jsou jen v prvním okamžiku determinovány příčinou, tj. dopady konkrétní pohromy, která je vyvolala. Poté jsou determinovány dobou, po kterou trvají a rozsahem zasažené organizace.
3. V případě, že dojde k významnému zdržení v nastartování vhodné odezvy na pohromu, dochází ke kritické situaci, která může mít až katastrofické dopady, protože v důsledku domino efektů vznikají další a další řetězce nežádoucích jevů.
4. Plány rychle zastarávají, a proto jsou nezbytné pravidelné aktualizace a testování.
5. Bezpečnost, odolnost či zranitelnost každého systému je vždy daná nejslabším prvkem, vazbou či tokem organizace.

Plánování bezpečné organizace proto vyžaduje bezpodmínečně interdisciplinární přístup vycházející a navazující na koncept lidské bezpečnosti (společnost je posedlá strachem z narušení bezpečnosti, protože současná společnost je složitá a velmi zranitelná) a udržitelného rozvoje (ekologická odpovědnost má vztah k environmentální bezpečnosti, ekonomická účinnost souvisí s ekonomickou a technologickou bezpečností, sociální solidarita je odrazem sociální a zdravotní bezpečnosti atd.).

V případě, ve kterém neexistuje účinná obrana organizace před pohromou, je nutností být připraven. To znamená, že organizace musí mít připraveny postupy, jimiž se musí zajistit odezva na situaci zaměřená na stabilizaci zasažené části organizace a obnova kritických procesů a zdrojů pro jejich realizaci. Nouzové plánování neomezuje rizika a musí být na míru toho, kdo provádí odezvu i navazující obnovu. V žádném případě nejde o levnou záležitost. Jde o zajištění uspořádání souboru znalostí a o prosazení, že každá odpovědně řízená instituce bude mít bezpečnostní koncepci. Ta musí vycházet z klasifikace nouzových situací a z analýzy rizik zaměřené na zjištění očekávání, jaké dopady a jak jsou pravděpodobné při vzniku pohromy o očekávané (právně definované) velikosti.

Plánování je spolehlivé, když postupy:

- vedou k cíli pomocí optimálního způsobu, který lze zajistit disponibilními zdroji, silami a prostředky,
- jsou formalizované,
- obsahují opatření k omezení (zmírnění) dopadů,
- zajišťují kontinuální proces,
- umožní zvládnout možné situace,
- jsou multidisciplinární (tj. nejsou naivní a levné),
- respektují problémy v zajištění potřebných zdrojů, a proto s nimi neplýtvají,
- racionálně využívají bezpečnostní infrastrukturu.

Plány musí mít hierarchickou strukturu, protože hierarchické jsou jak procesy, tak zdroje. Nejčastěji se používají tři úrovně, a to:

1. Analýza rizik, která stanovuje strategická pravidla:
   - základní klasifikace klíčových procesů a zdrojů a jejich zabezpečení,
   - plán zachování funkčnosti.
2. Zajištění dat a informací a odvození znalostí a návrh cílů.
3. Seznam konkrétních realizačních opatření a návrh postupů na jejich realizaci (lze využít nástroje multikriteriálního rozhodování, např. metoda kritické cesty, Petriho sítě, optimalizační metody síťové analýzy apod.) [16].

Musíme si uvědomit, že např. proces zvládnutí nouzové situace v organizaci probíhá v jistém, opakujícím se životním cyklu:

1. Normální podmínky / provoz organizace, tj. žádná pohroma.
2. Reakce na vznik nouzové situace vyvolané výskytem pohromy.
3. Obnova základních funkcí organizace.
4. Prozatímní provoz organizace.
5. Obnova plného provozu organizace.
6. Normální provoz organizace po obnovení plné funkce.

Obnova plného provozu znamená přechod z nouzového provozu organizace na plný provoz. Obvykle je nejvíce opomíjená.

Dalším příkladem je formální postup pro proces zvládání konkrétní nouzové situace, který je vždy v hlavních rysech tento:

- analýza rizik,
- zjištění dopadů, zranitelností a jejich ocenění,
- stanovení kritických procesů a zdrojů potřebných pro jejich realizaci,

- stanovení doby, za kterou musí být kritické procesy obnoveny, aby nedošlo k další eskalaci nouzové situace vyvolané pohromou. Jde totiž o to, aby příliš dlouho nepůsobila spřažení vzniklá v organizaci v důsledku vnitřních vazeb, obrázek 8.

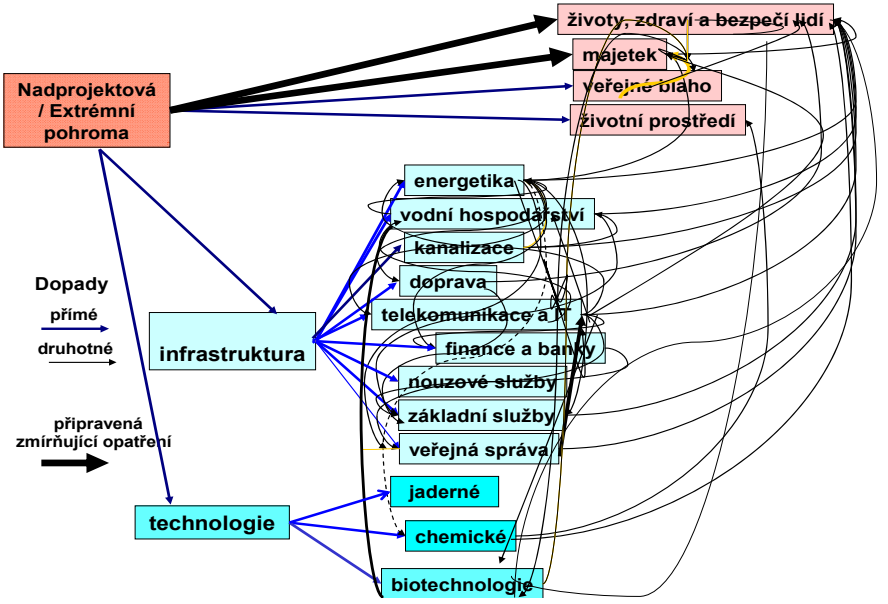
Obrázek 8 ukazuje vliv selhání kritické infrastruktury při nadprojektových pohromách. Vyznačené složité vazby, tzv. „interdependences" jsou předmětem výzkumu EU v rámci Sedmého rámcového programu. Obrázek 8 ukazuje, že v případě výskytu nadprojektové pohromy (tj. pohromy proti které se již nedělají nadstandardní preventivní opatření v územním plánování, projektování, výstavbě a provozování objektu, infrastruktury, v systému péče o zdraví, bezpečí, životní prostředí a veřejné blaho) jsou vybudovány ochranné systémy v rámci nouzového a krizového řízení pro bezpečnost jen vybraných chráněných zájmů (životy a zdraví lidí a majetek). Je proto nutno zdůraznit, že v doposud vybudovaném systému ochrany nejsou dostatečně zohledněny vnitřní vazby jdoucí napříč organizací a jejím okolím. Tento problém je třeba v zájmu bezpečnosti a rozvoje organizace vyřešit, tj. odstranit a nebo alespoň snížit na žádoucí úroveň druhotné dopady v řetězcích dopadů, které souvisí s výskytem konkrétních pohrom [2,3,17].

Pro každý kritický proces se nejprve pro potřeby řízení musí určit možné scénáře. Za vše odpovídá vrcholový management. Plán je ***komplexní obrázek o procesech a jejich závislostech.*** Plán má proto ***řešit problémy, porozumět budoucím situacím, formulovat priority a stanovit odpovědnosti***. Nástroje řízení, které stanovuje plán jsou:

- soustava indikátorů,
- monitoring,
- cíle.

Podle těchto nástrojů jsou nastaveny všechny další části řízení. Když je plán formální, tak řízení je bezbřehé a není zajištěno dosažení cílů. Proto při každém plánování si je třeba uvědomit, že prostorové uspořádání, funkční využívání organizace i předurčení chování lidí je komplexní proces pro zajištění vzájemného souladu požadavků hospodářských a jiných činností.

Plánování v organizaci založené na stanovení cílů, odstranění možných problémů a na ceně, kterou organizace zaplatí za selhání, je zvláště nutné zaměřit se na životy lidí, životní prostředí a ten majetek, který nejvíce vyžaduje investice a sledovat dopady na vazby mezi prvky a vazby napříč celého systému infrastruktury. Poslední výzkumy ukazují, že zvláště důležité je sledovat spletitost vnitřních závislostí napříč kritickou infrastrukturou. Při znázornění organizace jako systému se zjistí, že některé prvky, vazby či toky jsou vysoce zásadní pro stabilitu, kontinuitu a rozvoj organizace. V těchto případech je nutno v zájmu bezpečnosti provést specifická opatření a tyto prvky, vazby či toky speciálně zodolnit a případně zálohovat, a to i několikrát (např. u jaderných elektráren, jež jsou v provozu v České republice je zálohování 300 %). To také platí pro dodávky kritického materiálu nebo pro zajištění kritických služeb (např. záložní zdroje elektrické energie).



Obr. 8
Dopady extrémních pohrom (živelních či jiných)

Základním nástrojem pro plánování i řízení jsou procesní modely. Ty umožňují sestavit postupy a scénáře pro určité situace, které mají určité podobné rysy. Jsou vhodné pro plánování i pro odezvu a obnovu. Modely se sestrojují na základě konkrétních potřeb. *Základem jejich každé aplikace je požadavek, že k tomu, aby daly správný výsledek, musí být splněny předpoklady, na jejichž základě byly vytvořeny.* Výsledkem aplikace procesních modelů jsou normy, standardy, havarijní, nouzové, krizové a jiné plány, scénáře pohrom, scénáře odezvy, scénáře obnovy apod.

7. Systém řízení bezpečnosti organizace

Protože zdrojů, sil a prostředků má vždy každá organizace nedostatek, tak pro řízení bezpečnosti je nutno se soustředit na priority. V první řadě to znamená na základě velikosti ohrožení od konkrétní pohromy a zranitelnosti organizace vůči konkrétní pohromě rozdělit existující pohromy do následujících skupin:

- pohromy, které nemohou mít dopady na organizaci,
- pohromy, které mají jen přijatelné dopady na organizaci, pro které používáme označení pohromy relevantní,

- pohromy, které mají v organizaci takové dopady, které jsou zvládnutelné při provedení připravených preventivních a zmírňujících opatření, pro které používáme označení pohromy specifické,
- pohromy, které mají v organizaci nepřijatelné dopady, a tudíž je nutné provést zásadní preventivní opatření v oblasti technické, organizační, právní i vzdělávací a je nutné mít možnost aktivovat všechna zdroje a prostředky na zvládnutí jejich dopadů a nastartování dalšího rozvoje, pro které používáme označení pohromy kritické. Tyto vyvolají nebo mohou vyvolat krizové situace.

Problémové oblasti při řízení bezpečnosti jsou:

1. Ve kterém místě / kterém sektoru se pohromy v organizaci a jejím okolí mohou vyskytnout a jak jsou při výskytu pohromy v organizaci rozloženy jejich dopady?
2. Jaké pohromy se v organizaci mohou vyskytnout a jaké mají dopady?
3. Za jakých podmínek se pohromy v organizaci mohou vyskytnout a jaké podmínky mohou způsobit eskalaci jejich dopadů?
4. Jak často se pohromy v organizaci mohou vyskytnout?
5. Od jaké velikosti mají pohromy na organizaci nežádoucí, tj. nepřijatelné dopady, které působí škody na chráněných zájmech, tj. i na majetku?
6. Jaká je maximální možná (očekávaná) velikost pohromy v dané organizaci?
7. Jaké škody na majetku může vyvolat maximální možná pohroma určená na specifikované hladině věrohodnosti v organizaci a jaké jsou její dopady na lidi, životní prostředí, majetek a ostatní chráněné zájmy organizace?
8. Co se proti nežádoucím dopadům pohrom dá dělat v organizaci na úseku bezpečnostního plánování, projektování, výstavby a provozu občanských i technologických objektů a infrastruktury a popř. v dalších oblastech jako jsou monitoring, inspekce, vzdělání aj., aby se zabránilo výskytu pohrom, kterým lze zabránit nebo aby se zabránilo jejich vysoce nepřijatelným dopadům a nebo alespoň, aby se nepřijatelné dopady v případě výskytu zmírnily preventivními opatřeními, připraveností, vhodnou odezvou na pohromu a obnovou, při níž bude respektována prevence ztrát a cíle udržitelného rozvoje?
9. Jaká opatření vůči konkrétním pohromám v organizaci jsou žádoucí v oblasti technické, organizační, finanční, sociální, právní, vzdělání a výchovy?
10. Jaká nepřijatelná a zbytková rizika (tj. nežádoucí dopady s pravděpodobností výskytu vyšší než stanovená mez) s ohledem na možné pohromy v organizaci zůstanou, když se provedou racionální opatření, která může organizace zajistit v oblasti technické, organizační, finanční, sociální, právní, vzdělání a výchovy?
11. Jak provádět odezvu na pohromu, jaké jsou její priority, kritická místa apod.?
12. Jak provádět obnovu majetku po pohromě v organizaci, aby se racionálně využily zdroje, síly a prostředky, aby se zamezilo dalším ztrátám, aby se zvýšila odolnost proti pohromám a aby se nastartoval další rozvoj organizace se všemi položkami (majetkem, životním prostředím, infrastrukturou, službami apod.), na nichž je organizace závislá?
13. Jaká forma řízení a provádění obnovy majetku po pohromě v organizaci je vhodná a jak ji lze realizovat?

14. Jak vytvořit finanční rezervu organizace na racionální obnovu majetku po pohromě v organizaci?

Strategie pro zajištění bezpečí a udržitelného rozvoje organizace spočívá v:

- aplikaci systémového a pro-aktivního řízení, které se opírá o znalosti a zkušenosti získané pro organizaci z kvalifikovaných dat,
- kvalifikovaném vyjednávání s riziky ve prospěch bezpečí a udržitelného rozvoje organizace,
- vypořádání rizik pomocí prevence, zmírnění, pojištění, rezervy, připravenosti na odezvu a obnovu a sestavení plánu na zvládnutí nepředvídaných situací (contingency plan),
- aplikaci správného řízení, ve kterém jsou provázané řízení bezpečnosti, nouzové řízení a krizové řízení,
- sestavení programu na zvyšování bezpečnosti v území,
- stanovení měr na posuzování úrovně bezpečnosti ve smyslu účinnosti bezpečnostního systému (indikátory),
- naplnění programu provázanými projekty + naplnění projektů provázanými procesy,
- adresném přidělení úkolů a odpovědností všem zúčastněným,
- realizaci příslušných činností a opatření, která je spojená s kvalifikovaným a důsledným monitoringem,

Základním principem je kvalifikované propojení řízení oblastí technické, organizační, finanční, personální, sociální, znalostní; a jasné role a odpovědnosti všech zúčastněných. Systém řízení bezpečnosti organizace proto postihuje řadu oblastí, tj. technickou, vojenskou, legislativní, finanční, ekonomickou, sociální, ekologickou, vzdělávací, výzkumnou apod. Na úseku bezpečnosti a udržitelného rozvoje lidského systému mají z hlediska současného poznání a současných koncepcí sofistikovaných bezpečnostních systémů úkoly všichni zúčastnění. Úkoly jednotlivých zúčastněných a jejich propojení v různých situacích stanoví právní předpisy, morální a jiné standardy a normy.

V rámci strategie pro zajištění bezpečí a udržitelného rozvoje organizace [2] musí být:

- sestaven program na zvyšování bezpečnosti v organizaci,
- míry pro posuzování úrovně bezpečnosti ve smyslu účinnosti bezpečnostního systému (indikátory),
- program na zajištění bezpečnosti naplněný provázanými projekty,
- projekty naplněné provázanými procesy.

Nástroje správy organizace, které zajišťují bezpečí a rozvoj systému, tj. jinými slovy zachování či ochranu a rozvoj chráněných zájmů [2,13], jsou:

- provázaný systém řízení (strategické, taktické i operativní) založené na kvalifikovaných datech, odborných hodnoceních a správných metodách rozhodování,
- výchova a vzdělání zaměstnanců,
- věda, výzkum a TSO / odborné organizace zajišťující odbornou podporu organizaci,
- specifická výchova technických a řídících pracovníků,

- technické, zdravotnické, ekologické, společenské, kybernetické a jiné standardy, normy a předpisy, tj. nástroje pro regulaci procesů, které mohou nebo by mohly vést k výskytu (vzniku) pohromy nebo k zesílení jejich dopadů,
- inspekce,
- systém spolupráce s veřejnou správou, s organizacemi v území a s organizacemi používajícími podobné technologie,
- výkonné složky ke zvládnutí nouzových situací,
- systémy ke zvládnutí kritických situací (řízení kontinuity, krizové řízení),
- bezpečnostní, nouzové a krizové plánování.

Aby řízení bylo správné, je nutné nástroje kvalifikovaně používat. To znamená:

- používat podklady získané na základě kvalifikovaných dat, která splňují požadavky na reprezentativní datové soubory (úplnost, ocenění nejistot, vypořádání se s neurčitostmi v datech pomocí specifických matematických přístupů),
- aplikovat správné metody rozhodování, které jsou adekvátní problému, o kterém se rozhoduje.

To znamená, že pro:

- strategické řízení organizace, které je zaměřené na řízení bezpečnosti, je nutné ***používat ověřené datové soubory, ověřené metody pro zpracování dat a ověřené metody pro rozhodování***,
- střednědobé řízení organizace, které je zaměřené na připravenost směrovanou na zvládnutí problémů spojených s nouzovými situacemi (povodně, havárie apod.) v organizaci, je možno používat ***méně přesná data, metody zpracování dat i metody rozhodování*** (méně přesné procesní modely, software, odhady apod.), protože každá nouzová situace je jedinečná kvůli proměnným podmínkám při jejím vzniku a změnám v disponibilitě zdrojů, sil a prostředků organizace na reakci,
- operativní řízení, kdy se rozhoduje v časové tísni a při nedostatku dat (odezva), je nutno ***na základě cíleně získaných znalostí a zkušeností použít naučené a procvičené postupy*** (zpracované např.formou případových studií), protože rychlá reakce je žádoucí.

Systém řízení bezpečnosti (tzv. SMS – Safety Management System) organizace zahrnuje organizační strukturu, odpovědnosti, praktiky, předpisy, postupy a zdroje pro určování a uplatňování prevence pohrom či alespoň zmírnění jejich nepřijatelných dopadů v území. Zpravidla se týká řady otázek, kromě jiného i organizace, pracovníků, identifikace a hodnocení ohrožení a z nich plynoucích rizik, řízení chodu organizace, řízení změn v organizaci, nouzového a krizového plánování, monitorování bezpečnosti, auditů a přezkoumávání [2]. Na základě citované práce SMS organizace se skládá z oblastí:

1. Oblast koncepce a řízení, která se dále dělí na podoblasti:
   - podoblast celkové koncepce,
   - podoblast dílčích cílů bezpečnosti,
   - podoblast vedení / spravování bezpečnosti,

- podoblast systému řízení bezpečnosti,
- podoblast personálu, která se dále dělí na úseky:
  * úsek řízení lidských zdrojů,
  * úsek výcviku a vzdělání,
  * úsek vnitřní komunikace / informovanosti,
  * úsek pracovního prostředí,
- podoblast revize a hodnocení plnění cílů v bezpečnosti.

2. Oblast administrativních postupů, která se dále dělí na podoblasti:
   - podoblast identifikace ohrožení od možných pohrom a hodnocení rizika,
   - podoblast dokumentace,
   - podoblast postupů (včetně systémů pracovních povolení),
   - podoblast řízení změny,
   - podoblast bezpečnosti ve spojení s kontraktory,
   - podoblast dozoru nad bezpečností výrobků.
3. Oblast technických záležitostí, která se dále dělí na podoblasti:
   - podoblast výzkumu a vývoje,
   - podoblast projektování a montáže,
   - podoblast inherentně bezpečnějších procesů,
   - podoblast průmyslových standardů,
   - podoblast skladování nebezpečných látek,
   - podoblast údržby integrity a údržby zařízení a objektů.
4. Oblast vnější spolupráce, která se dále dělí na podoblasti:
   - podoblast spolupráce se správními úřady,
   - podoblast spolupráce s veřejností a dalšími zúčastněnými (včetně akademických pracovišť),
   - podoblast spolupráce s dalšími podniky.
5. Oblast nouzové připravenosti a odezvy, která se dále dělí na podoblasti:
   - podoblast plánování vnitřní (on-site) připravenosti,
   - podoblast usnadnění plánování vnější (off-site) připravenosti (za kterou odpovídá veřejná správa),
   - podoblast koordinace činností resortních organizací při zajišťování nouzové připravenosti a při odezvě.
6. Oblast zpráv a šetření havárií / skoro nehod, která se dále dělí na podoblasti:
   - podoblast zprávy o haváriích, skoro nehodách a dalších poučných zkušenostech,
   - podoblast vyšetřování,
   - podoblast odezvy a následné činnosti po nehodách (včetně aplikace poučení a sdílení informací).

Systém řízení bezpečnosti organizace se opírá o koncepce prevence pohrom či alespoň jejich závažných dopadů, která zahrnuje povinnost zavést a udržovat systém řízení, ve kterém jsou zohledněny dále uvedené problémy:

a) role a odpovědnosti osob podílejících se na řízení závažných ohrožení od pohrom na všech organizačních úrovních a opatření na zajištění výcviku, která jsou sladěna s identifikovanými potřebami výcviku,

b) plány pro systematické identifikování závažných ohrožení od pohrom a z nich plynoucích rizik, která jsou spojena s normálními a abnormálními podmínkami, a pro hodnocení jejich pravděpodobnosti a krutosti (velikosti),
c) plány a postupy pro zajištění bezpečnosti všech komponent a funkcí v území, a to včetně údržby objektů, zařízení,
d) plány na implementaci změn v území, objektech i zařízeních,
e) plány na identifikaci předvídatelných nouzových situací systematickou analýzou, včetně přípravy, testů a posuzování nouzových plánů pro odezvu na takové nouzové situace,
f) plány pro probíhající hodnocení souladu s cíli vyjasněnými v koncepci bezpečnosti a SMS a mechanismy pro vyšetřování a provádění korekčních činností v případě selhání s cílem dosáhnout stanovené cíle,
g) plány na periodické systematické hodnocení koncepce bezpečnosti, účinnosti a vhodnosti SMS a kritéria pro posuzování úrovně bezpečnosti vrcholovým týmem pracovníků.

Bezpečnost je záležitostí všech zúčastněných, tj. vedoucích pracovníků, zaměstnanců i náhodně přítomných. V těchto souvislostech se mluví o ***tzv. zlatých pravidlech všech zúčastněných*** [2], kterými jsou:

- dle svých možností preventivními opatřeními zabránit vzniku pohrom a nebo alespoň jejich nepřijatelným dopadům, zajistit připravenost na zvládnutí nepřijatelných dopadů na chráněné zájmy organizace a účinnou odezvu organizace,
- komunikovat a spolupracovat s ostatními zúčastněnými ve všech aspektech prevence, připravenosti a odezvy organizace,
- znát ohrožení od pohrom a možná rizika v organizaci a jejím okolí v území i objektu,
- implementovat a respektovat „kulturu bezpečnosti“, která je respektována a prosazována všemi zúčastněnými za všech okolností,
- zřizovat systémy řízení bezpečnosti, sledovat a popř. korigovat jejich činnost,
- používat principy inherentní bezpečnosti při navrhování, projektování a provozování objektů a jejich zařízení,
- pečlivě řídit změny v organizaci,
- být připraven na zvládnutí všech pohrom, které mohou nastat,
- pomáhat ostatním zúčastněným při vykonáváni jejich rolí a odpovědností,
- provádět neustálé vylepšování bezpečnosti,
- pracovat ve shodě s kulturou bezpečnosti, bezpečnými postupy a výcvikem,
- usilovat neustále o veškerou informovanost a poskytovat informace a pro řídící pracovníky zajišťovat zpětnou vazbu,
- usilovat o rozvoj, posilování a ustavičné zlepšování koncepce bezpečnosti, předpisů a směrnic,
- vést a motivovat všechny další zúčastněné k tomu, aby plnili své úlohy a odpovědnosti,
- znát rizika uvnitř sféry vlastní odpovědnosti, příslušně plánovat opatření pro jejich správné řízení,
- používat vhodnou a koherentní politiku plánování a následných činností,

- být si vědom rizik v organizaci a vědět co činit v případě jejich realizace,
- účastnit se nouzového plánování a odezvy.

8. Program na zvyšování bezpečnosti organizace

Účinná kultura bezpečnosti je základním prvkem bezpečnosti. Odráží koncepci bezpečnosti a vychází z hodnot, stanovisek a jednání vrcholových řídících pracovníků organizace a z jejich komunikace se všemi zúčastněnými. Je zřetelným závazkem aktivně se podílet na řešení otázek bezpečnosti a prosazuje, aby všichni zúčastnění konali bezpečně a aby dodržovali příslušné právní předpisy, standardy a normy. Pravidla kultury bezpečnosti musí být zapracována do všech činností v organizaci. Jejich základem není koncentrace na potrestání viníků / původců chyb, ale poučení z chyb a zavedení takových nápravných opatření, aby se chyby nemohly opakovat nebo aby se alespoň výrazně snížila četnost jejich výskytu.

Nástrojem pro zajištění bezpečné organizace, tj. takové organizace, ve které je účinná kultura bezpečnosti, je program na zvyšování bezpečnosti organizace [2]. Postup pro vytváření programu na zvyšování bezpečnosti organizace se skládá z dále uvedených kroků:

1. Definovat úkoly (dílčí cíle) a strategické cíle organizace s ohledem na bezpečnost.
2. Pro každý úsek organizace vybrat vhodné cílové a průběžné indikátory pro posuzování úrovně bezpečnosti.
3. Vytvořit slovník pro potřeby řízení integrální bezpečnosti.
4. Sladit standardy, metody dobré praxe a místní postupy.
5. Upravit seznam cílových indikátorů dle podmínek v předmětné organizaci.
6. Upravit seznam průběžných indikátorů dle podmínek v předmětné organizaci.
7. Stanovit způsob vyhodnocení cílových indikátorů (tj. hodnotový systém) dle podmínek v předmětné organizaci.
8. Stanovit způsob vyhodnocení průběžných indikátorů (tj. hodnotový systém) dle podmínek v předmětné organizaci.
9. Stanovit způsob / stupnici pro měření souboru indikátorů (tj. systém hodnot) a mezní limity dle podmínek v předmětné organizaci.

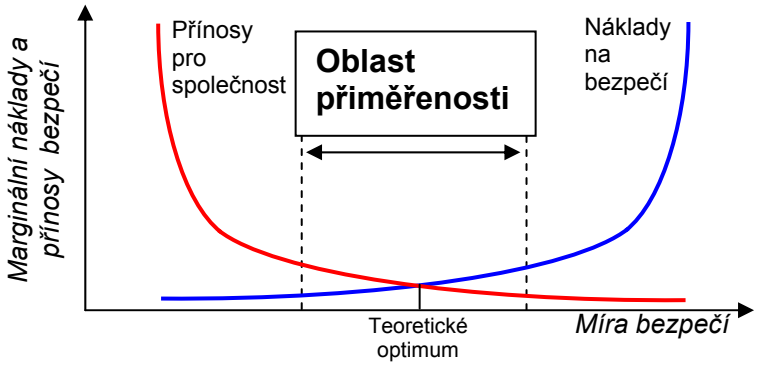
V praxi to znamená, že se pro každý úsek ve vybrané působnosti určí cílové a průběžné indikátory, které mají formu limitů a kontrolních seznamů [2]. K nim jsou v praxi přiřazená kritéria na vyhodnocení a stupnice pomocí nichž se určuje, kdy je cíle dosaženo a kdy ne.

9. Přiměřené náklady na bezpečnou organizaci

Na základě skutečností uvedených v odstavci 2 jsou náklady na zajištění bezpečí a udržitelného rozvoje organizace souhrnné náklady vynaložené na

vyjednávání s riziky. Tj. jsou to náklady na opatření a činnosti prevence, připravenosti, odezvy a obnovy, náklady na pojištění a rezervní náklady na nepředvídané situace vyvolané např. málo pravděpodobnou kumulací nežádoucích jevů. Z hlediska účinnosti jsou nejefektivnější náklady na prevenci [13]. Jsou však nákladné na znalosti, zdroje, síly a prostředky, jejich výsledek není okamžitě viditelný a je zřejmý až v budoucnosti po pohromě, a proto jejich aplikaci je správa organizace obvykle nakloněna jen v období po velké pohromě. Z důvodů zajištění ochrany a udržitelného rozvoje je proto nutné právně prosadit vynutitelnost zásadních preventivních opatření právními předpisy.

Při zajištění přijatelné úrovně bezpečí v organizaci, které v sobě inherentně obsahuje dostatečnou úroveň udržitelného rozvoje nelze zanedbat skutečnost, že zdroje každé organizace jsou omezené a že každá činnost i opatření vyžaduje zdroje, síly a prostředky. Proto možná úroveň bezpečí odpovídá stavu organizace, ve kterém mezní náklady na prevenci se rovnají mezním nákladům na odstranění škod (tj. nákladům na odezvu a obnovu). Lze konstatovat, že takto definovaná úroveň bezpečí je ekonomickým optimem pro organizaci [2], obrázek 9. Teoretické optimum pochopitelně není obecně platné, platí pro konkrétní organizaci, protože podmínky i zdroje, síly a prostředky organizace jsou proměnné. Oblast přiměřenosti pak určuje správa organizace, která buď přímo v oblasti své působnosti nebo prostřednictvím právních předpisů vyžaduje od ostatních zúčastněných realizaci určitých činností a opatření vedoucích k zajištění bezpečí zahrnujícího udržitelný rozvoj. Pochopitelně správné řízení může provádět jen kvalifikovaná správa a jen na základě disponibilních zdrojů.



Obr. 9
Bezpečí chápané jako ekonomické optimum pro organizaci

Dnes jsou již kvalifikované postupy na identifikaci možných škod, možných ztrát i možné újmy v konkrétní organizaci při jednotlivých pohromách (metodiky používané Swiss Re, Munich Re a další popsané v práci [13])

v závislosti na tom, jaké chráněné zájmy v organizaci jsou a jaké jsou zranitelnosti dané organizace. Jsou i postupy na vyčíslení nákladů na činnosti spojené s vyjednávání s riziky, a proto je možné podle zdrojů, sil a prostředků konkrétní organizace předurčit úroveň bezpečí zahrnující udržitelný rozvoj, které je v okolí teoretického optima. Z toho je rovněž zřejmé, že bohaté organizace mají predispozici zajistit vyšší úroveň bezpečí včetně udržitelného rozvoje než organizace chudé, mezi které patří i organizace ekonomicky bohaté, které se však soustřeďují jen na ekonomický růst a přehlížejí ostatní potřeby dnes i v budoucnu.

10. Závěr

Výše uvedené údaje ukazují reálný pohled na svět, tj. i když organizace bude mít nejlepší snahu zajistit nejlepším způsobem bezpečí zahrnující udržitelný rozvoj, tak musí správně vynakládat zdroje, síly a prostředky, protože možnosti každé organizace jsou omezené. *Vyjednávání s jakýmkoliv rizikem* je spojeno se zvyšováním nákladů, s nedostatkem znalostí, technických prostředků, kvalifikovaných lidí apod. Proto se v praxi hledá hranice, na kterou je únosné snížit riziko tak, aby vynaložené náklady byly ještě rozumné. Optimálně je třeba při vyjednávání s riziky také zvolit místně specifické přístupy, protože disponibilita zdrojů, sil a prostředků je rozdílná a mění se v čase. *Míra snížení rizika (určitá optimalizace) je většinou předmětem vrcholového řízení a politického rozhodování správy organizace*, při kterém se využívají současné vědecké a technické poznatky a zohledňují se ekonomické, sociální a další podmínky.

Zásadní obrat v řízení organizace s ohledem na žádoucí cíle nelze dosáhnout jednotlivými dílčími opatřeními, ale pouze komplexním přístupem s ohledem na místní podmínky. Složitá dělba kompetencí vede v praxi k vážným potížím a ve svém celku nepokrývá žádoucím způsobem celou problematiku. Pro zajištění bezpečí a udržitelného rozvoje organizace je třeba použít koordinovaný a cílevědomý přístup, který umožní postupně a v souladu s jejich důležitostí a naléhavostí řešit soubor úkolů ve všech sférách a součástech a docílit tak žádoucí stav organizace. Řešení problémů spočívá v oblasti investiční, technické, technicko-organizační, správní a řídící, vědeckovýzkumné, výchovy a dalších. Efektivní řešení problémů nelze zajistit bez strategického a koncepčního řízení, pro které musí připravit podrobné, objektivní a systematické údaje výzkum. Operativní přístup při řešení problémů bez navázání na strategické plány obvykle není správným řešením ve střednědobém a dlouhodobém výhledu.

Résumé

To ensure the safe organisation with a potential of sustainability development, it is necessary:

- *to know and to consider all possible risks inside and outside organisation, namely in details and in connectedness,*
- *to negotiate with risk aright,*

- *to determine the risk management aright,*
- *to use qualified tools for the risk management in the benefit of safety, i.e. security and sustainable development.*

From the professional view of present knowledge there is necessary to understand that the organisation is an open system, the behaviour and the state of which are influenced by processes and phenomena being under way inside and outside of system. Their impacts are modified by a complicated net of links and flows being within partial systems, across all system and in the vicinity of organisation. In the face of it the risk management must be complex and its priorities must be directed to security and sustainable development of organisation. Because sources, forces and means of each organisation are limited and its accessibility is also dependent on conditions being in organisation vicinity, the organisation management must competently handle with them in order that required aims might be reached.

Literatura

[1] PROCHÁZKOVÁ, D. Principles of Good Governance of Public Affairs with regard to Security. In *Security and Safety Management and Public Administration (Proceedings of International Scientific Conference 16. – 19. 9. 2008)*. Praha: Police Academy of the Czech Republic, s. 266-275. ISBN 978-80-7251-289-8.

[2] PROCHÁZKOVÁ, D. *Strategie řízení bezpečnosti a udržitelného rozvoje území*. Praha: PA ČR, 2007. 203 p. ISBN 978-80-7251-243-0.

[3] PROCHÁZKOVÁ, D. *Bezpečnost lidského systému*. Ostrava: SPBI, 2007. 139 p. ISBN 978-80-86634-97-5.

[4] REES, W. E. Economic, Ecolog, and the Role of Environmental Assessment in Achieving Sustainable Development. In P. JACOBS, B. SADLER (eds). *Sustainable Development and Environmental Assessment: Perspectives on Planning for a Common Future*. Ottawa: CEARC, 1989, p. 123-141.

[5] DEVUYST, D. Sustainaability Assessment: the Application of a Methodological Framework. In *Proceedings of the 19th Annual Meeting of the International Association for Impact Assessment*. Glasgow, 15-20 June 1999, 37 p.

[6] HARDI, P., T. Zdan. *Assessing Sustainable Development. Principles in Practice*. Winnipeg: Intenational Institute for Sustainable Development, 1997.

[7] PROCHÁZKOVÁ, D. *Bezpečnost a krizové řízení*. Praha: POLICE HISTORY, 2006. 255 p. ISBN 80-86477-35-5.

[8] BUSELICH, K. *An Outline of current Thinking on Sustainability Assessment.* Western Australia: Institute for Sustainability and Technology Policy, Murdoch University, 2002. Dostupný z WWW: <http://wwwistp.murdoch, edu.au>.

[9] URL: *Sustainability*. http://www.centerforsustainablecities.com.

[10] PROCHÁZKOVÁ, D. *Podmínky udržitelného rozvoje krajiny a lidských sídel, kritické prvky a příslušná kritéria*. [Odborná zpráva č. 4 k projektu MZe 1R56002]. Praha: CITYPLAN spol. s r.o., 2007. 255 p.

[11] WALKER, T. Resilience Management in Social-ecological System. *Conservation Ecology*, 6(1), 2002. Dostupný z WWW: <http://www.consecol.org >.

[12] NEEFJES, K. *Environments and Livelihoods - Strategies for Sustainability*. *Development Guidelines*. Oxford: Oxfam Publication, 2000.

[13] PROCHÁZKOVÁ, D. *Metodika pro odhad nákladů na obnovu majetku v územích postižených živelní nebo jinou pohromou*. Ostrava: SPBI SPEKTRUM XI, 2007. 251 p. ISBN 978-80-86634-98-2.

[14] PROCHÁZKOVÁ, D. Safety, Security and Risk. In *Security and Safety Management and Public Administration (Proceedings of International Scientific Conference 16. – 19. 9. 2008)*. Praha, 2008, p. 276-285. ISBN 978-80-7251-289-8.

[15] PROCHÁZKOVÁ, D. *Územní, nouzové a krizové plánování*. České Budějovice: VŠERS, 2009. 204 p. ISBN 978-81-86623-2.

[16] PROCHÁZKOVÁ, D. Zprávy k projektu MZe:
Teoretický rozbor problému, analýza a kritický rozbor současného stavu v České republice i ve světě a používané odborné postupy. [Odborná zpráva č. 1 k projektu MZe 1R56002]. Praha: CITYPLAN spol. s r.o., 2005. 82 p.
Analýza a kritický rozbor poznatků a kritické položky v krajině a lidských sídlech. [Odborná zpráva č. 2 k projektu MZe 1R56002]. Praha: CITYPLAN spol. s r.o., 2006. 289 p.
Kritéria pro udržitelný rozvoj a pomocný systém pro podporu rozhodování ve prospěch krajiny a lidských sídel. [Odborná zpráva č. 3 k projektu MZe 1R56002]. Praha: CITYPLAN spol. s r.o., 2006. 234 p.
Multikriteriální rozhodování, hledání zásad ve prospěch udržitelného rozvoje krajiny a identifikace kritických prvků v krajině. [Odborná zpráva č. 4 k projektu MZe 1R56002]. Praha: CITYPLAN spol. s r.o., 2007. 160 p.
Podmínky udržitelného rozvoje krajiny a lidských sídel, kritické prvky a příslušná kritéria. [Odborná zpráva č. 5 k projektu MZe 1R56002]. Praha: CITYPLAN spol. s r.o., 2007. 258 p.

[17] PROCHÁZKOVÁ, D. a BALOG, K. Management of Critical Infrastructure Safety. In *Security and Safety Management and Public Administration. (Proceedings of International Scientific Conference 16. – 19. 9. 2008).* Praha, 2008. p. 286-296.