STRATEGICKÉ ŘÍZENÍ BEZPEČNOSTI

STRATEGIC SAFETY MANAGEMENT

Dana PROCHÁZKOVÁ
prochazkova@fd.cvut.cz

Došlo 27. 3. 2013, upraveno 7. 6. 2013, přijato 13. 6. 2013.
Dostupné na http://www.population-protection.eu/attachments/046_vol5n2_prochazkova.pdf.

Abstract

The paper deals with the human system integral safety and with the human system safety management in the profit of security and sustainable development of humans. With regard to fact that safety level depends on a quality of tools for trade-off with risks, it specifies problems´ domains and it determines the strategy for management faced to ensuring the targets. It gives: safety management principles, i.e. principles of management of risks in the benefit of security and sustainable development of humans and the other assets that human essentially needs for life; general model of safety management system of real entities; and levels of problems solving used in theory and practice of management.

Key words

Security, sustainable development, safety, risk management, model of safety management system, problems solving levels.

ÚVOD DO PROBLEMATIKY INTEGRÁLNÍ BEZPEČNOSTI A JEJÍHO ŘÍZENÍ

Na základě dokumentů OSN, EU a odborné literatury je bezpečnost chápána jako soubor opatření a činností, kterými lidstvo zajišťuje své bezpečí a udržitelný rozvoj [1]. V daném pojetí se neorientuje jen na jedno chráněné aktivum, ale na celý komplex aktiv, které člověk potřebuje ke kvalitnímu životu. Komplex aktiv zahrnuje životy, zdraví a bezpečí lidí, majetek, veřejné blaho, životní prostředí, infrastruktury a technologie. Z uvedeného důvodu bezpečnost musí být chápána komplexně a vždy se musí dbát na skutečnost, aby opatření a činnosti prováděné na ochranu jednoho aktiva nezvyšovaly významně rizika aktiva jiného. Bezpečnost dílčí, která je vztažena jen k jednomu aktivu, se používá v praxi jen ve specifických případech. Podobně tak i bezpečnost integrovaná.

Pro řešení otázek spojených s bezpečím a udržitelným rozvojem lidí je třeba používat integrální bezpečnost, která v sobě obsahuje i opatření a činnosti vůči škodlivým jevům spojeným s vazbami a toky v systému, který představuje

sledovaná entita, tj. území, správní celek, podnik apod. Dle současného poznání spřažení vyvolaná nežádoucími materiálovými, informačními, finančními či jinými toky v entitě jsou příčinou kaskádovitých selhání, která vážně narušují existenci i činnost entity [2].

BEZPEČNÁ ENTITA A RIZIKA

Bezpečná entita je entita, ve které všechna chráněná aktiva, o které řídicí systém entity musí v zájmu své existence a svého rozvoje pečovat, jsou v bezpečí. Každá reálná entita je systém systémů, tj. skládá se z několika překrývajících se systémů (překrytí znamená vzájemnou závislost) [1-3]. Je bezpečná a má perspektivu udržitelného rozvoje jen tehdy, když je řízena jako systém systémů na základě kvalifikovaných dat a jestliže jsou zvažovány skutečnosti jako: rizika jsou existující realitou a v čase se objevují stále nová rizika, a proto je třeba žít podle správné koncepce život s riziky, kterou přijala OSN v r. 2005 [1].

Problémové oblasti při řízení rizik

Z dlouhodobého výzkumu pohrom ve světě, jehož výsledky jsou shrnuty v [1], problémové oblasti při každém řízení entity zaměřeném na rizika jsou:

1. Kde se pohromy ve sledované entitě a jejím okolí mohou vyskytnout a jak jsou ve sledovaném subjektu rozloženy jejich dopady?
2. Jaké pohromy se ve sledované entitě mohou vyskytnout a jaké mají dopady?
3. Za jakých podmínek se pohromy ve sledované entitě mohou vyskytnout a jaké podmínky mohou způsobit eskalaci jejich dopadů?
4. Jak často se pohromy ve sledované entitě mohou vyskytnout?
5. Od jaké velikosti mají pohromy na sledovanou entitu nežádoucí (nepřijatelné) dopady, které působí škody, ztráty a újmy na chráněných aktivech?
6. Jaká je maximální možná (očekávaná) velikost pohromy ve sledované entitě?
7. Jaké škody na chráněných aktivech může vyvolat maximální možná pohroma určená na specifikované hladině věrohodnosti ve sledované entitě a jaké jsou její dopady na chráněná aktiva ve sledované entitě?
8. Co se proti nežádoucím dopadům pohrom dá dělat ve sledované entitě na úseku bezpečnostního (strategického) 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 anebo alespoň, aby se nepřijatelné dopady na chráněná aktiva zmírnily preventivními opatřeními, připraveností, vhodnou odezvou na pohromu a obnovou, při níž je respektována prevence ztrát a cíle udržitelného rozvoje?
9. Jaká opatření vůči konkrétním pohromám ve sledované entitě 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 ve sledované entitě zůstanou, když se provedou racionální opatření, která může sledovaná entita 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 chráněných aktiv po pohromě ve sledované entitě, 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 entity se všemi položkami (majetkem, životním prostředím, infrastrukturou, službami apod.), na nichž je sledovaná entita závislá?
13. Jaká forma řízení a provádění obnovy chráněných aktiv po pohromě ve sledované entitě je vhodná a jak ji lze realizovat?
14. Jak vytvořit finanční rezervu ve sledované entitě na racionální obnovu chráněných aktiv po pohromě v entitě?

Nástroje pro vyjednávání s riziky

Na základě znalostí a historických zkušeností úroveň bezpečnosti každé entity je výsledkem vyjednávání s riziky. Základní nástroje uvedeného procesu tvoří:

- řízení / management (strategické, taktické i operativní) založené na kvalifikovaných datech, odborných hodnoceních a správných metodách rozhodování,
- výchova a vzdělání občanů,
- specifická výchova technických a řídících pracovníků,
- technické, zdravotnické, ekologické, kybernetické a jiné standardy, normy a předpisy, tj. nástroje pro regulaci procesů, které mohou nebo by mohly vést ke vzniku pohromy nebo k zesílení jejich dopadů,
- inspekce,
- výkonné složky ke zvládnutí nouzových a kritických situací,
- systémy ke zvládnutí kritických situací,
- bezpečnostní, nouzové a krizové plánování,
- specifický systém řízení pro zvládnutí kritických situací (v ČR se pro předmětný typ managementu používá označení krizové řízení; ve světě se mluví o řízení odezvy nebo o řízení pohrom).

Odedávna je známo, že když chceme nějaký jev řídit nebo se vůči němu bránit, tak musíme znát jeho příčinu, velikost, opakovatelnost a podstatu působení dopadů na chráněná aktiva.

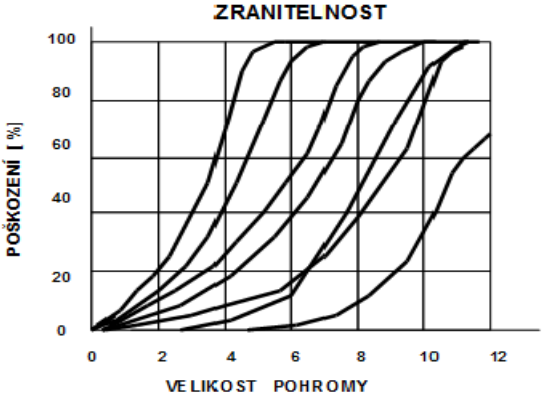
Aspekty strategického řízení

Na základě současného poznání se strategické řízení entit zaměřuje na dlouhodobou udržitelnost. Jeho cílem je integrita systémů, protože systémové služby zajišťují život podporující funkce. Považuje člověka za součást systému,

integruje lidskou činnost s ochranou přírodního prostředí a reaguje citlivě na potřeby lidí v kontextu ekosystémů a technologických systémů. V každém řídícím procesu je důležitou částí kvalitní a kvalifikované rozhodování, a proto je zapotřebí v rámci uplatňovaného systému strategického řízení vytvořit systémy na podporu rozhodování, poněvadž rozhodování vůči systémům je složité a musí mít vícedimenzionální charakter. V rozhodování se řeší dilemata:

- vztah mezi riziky a přínosy (často větší přínos pro lidi znamená zvýšené riziko pro ekosystémy),
- časový konflikt mezi současnými a budoucími potřebami,
- sociální konflikt (vztah potřeby jedince a celku).

Strategie řízení bezpečnosti představuje ucelenou sadu standardních, prakticky ověřených kroků a nástrojů k řízení změn a zároveň i samotný proces řízení předmětných změn. Vychází z poznání, že zvládnutí jakéhokoliv netriviálního procesu v systému není dílem okamžiku, ale je výsledkem zaměřeného působení souboru opatření a činností aplikovaných v prostoru a čase. Zahrnuje přesné určení žádoucího směru změn, stanovení přesného postupu jejich zavedení a průběžné sledování a vyhodnocování jejich průběhu a výsledků. Strategické plánování je pak nástroj, který se zaměřuje na to, aby řídící subjekt mobilizoval a co nejefektivněji využíval všechny vlastní zdroje, síly a prostředky a včas a správně reagoval na změny v okolním prostředí.



Obr. 1
Schematické znázornění křivek zranitelnosti objektů při různých pohromách vytvořené dle norem USA, UK, Německa a dalších [1]

Z pohledu řízení, jehož cílem je bezpečná entita s udržitelným rozvojem, je nejprve nutné znát procesy, děje i jevy, které narušují stanovený cíl. Potom si je nutné uvědomit logické vazby, tj. příčiny, následky a okolnosti, které hrají roli při realizaci následků příčin. Je to proto, že zásadní prevenci zajišťující účinnou

ochranu základních chráněných aktiv je třeba dělat proti příčinám. U následků ze stejného důvodu je pak možné provádět jen opatření a činnosti, které vedou ke zmírnění ztrát, škod a újmy na chráněných aktivech a které umožní obnovu a opětovné nastartování rozvoje žádoucím směrem. V rámci evropského projektu FOCUS [6] byly posouzeny závažnosti jak dlouhodobě sledovaných pohrom, tak nových pohrom, jako jsou selhání infrastruktur, korupce, klimatická změna apod.; rovněž byly identifikovány nové plíživé pohromy na území Evropy, např. zasolená zemědělská půda, klesající hladina podzemní vody, geomagnetické bouře apod.; celkem bylo sledováno více než sto pohrom, které jsou závažné pro obyvatele Evropy a světa.

Závažnost nouzové situace, kterou pohromy v dané entitě vyvolávají, závisí jednak na velikosti pohrom a jednak na zranitelnosti aktiv v předmětné entitě. Příklad křivek zranitelnosti je na obrázku 1.

ŘÍZENÍ BEZPEČNOSTI

Každé řízení bezpečnosti představuje řízení rizik, které je soustředěné na bezpečí a rozvoj, a proto vyžaduje systémový přístup. Systémový přístup je aplikace metody, techniky či postupu, při které zvažujeme vnitřek i vnějšek entity (tj. prvky, vazby a toky systému a jeho okolí). Pro odvození podkladů se používají prognostické metody, které směřují do budoucnosti a opírají se o časové řady extrapolace, trendy apod., expertní metody pro hodnocení a oceňování, odhady, kvantifikace, užití škál. Jejich aplikace při řízení bezpečnosti je možná jen někdy, protože chybí potřebné časové řady, které mají dobrou vypovídací schopnost pro řízení bezpečnosti [3]. Kvůli velké spletitosti poznatků se při sledování souvislostí v praxi používají často heuristiky, tj. metodologické způsoby objevování nových poznatků, práce s pramenným materiálem, získávání pramenů, třídění a hodnocení, hledání nových postupů a metod, řešení problémů. Heuristické metody jsou smíšené empiricko-intuitivní a exaktní metody, využitelné v oblasti měkkých systémů, které mají dva cíle, a to hledání podstaty problému a podpora tvořivého myšlení. Vyžadují schopnost práce s informacemi. Zaměření heuristik je obvykle na tvorbu variant, hledání podstaty problémů a na jejich řešení. Nejdůležitější heuristiky jsou brainstorming, brainwriting, analogie, metafora, obrazová a myšlenková schémata, meditace, cílený vhled.

Řízení bezpečnosti je typ řízení rizika, který v sobě zahrnuje princip předběžné opatrnosti, což znamená, že se neomezuje jen na rizika, jejichž míra (pravděpodobnost) výskytu je větší než normativně stanovená hodnota (obvykle 0.05), ale zvažuje i rizika, jejichž pravděpodobnost výskytu je velmi malá až zanedbatelná dle obvyklých měřítek, ale s nimi spojené nepřijatelné dopady jsou katastrofické alespoň pro jeden ze základních chráněných aktiv. Evropská komise stanovila konkrétní případy, ve kterých se má používat princip předběžné opatrnosti. Jde o případy, kdy: jsou vědecké údaje nedostatečné, neprůkazné nebo nejisté; a z předběžného vědeckého hodnocení vyplývá, že se lze důvodně obávat potenciálně nepřijatelných dopadů na zdraví lidí, zvířat a rostlin. Stanovila tři

pravidla, která jsou potřebná při uplatnění principu předběžné opatrnosti. Jejich aplikace znamená, že princip předběžné opatrnosti lze použít jen tehdy, když budou u sledovaného problému provedeny dále uvedené kroky:

- komplexní vědecké vyhodnocení provedené nezávislým odborným akreditovaným subjektem s cílem stanovit stupeň vědecké nejistoty,
- hodnocení potenciálních rizik a dopadů, které se mohou realizovat v případě, že se problém nebude řešit,
- účast všech zainteresovaných stran (za podmínek maximální průhlednosti) na studiu možných opatření.

Princip předběžné opatrnosti de facto říká, že vždy, když existuje riziko, se kterým jsou spojené možné ztráty, škody nebo újmy, je třeba jednat tak, jako by dané ztráty, škody či újmy byly reálné. A to i v případě, že riziko není zcela stoprocentně ověřené. Dobrým příkladem je např. problém globálního oteplování. Vědci se často neshodují na velikosti ohrožení od zmíněného jevu a na jeho dopadech pro planetu. Přesto Evropská unie podle principu předběžné opatrnosti se snaží jednat tak, aby zabránila rizikům, plynoucím z globálního oteplování podle nejkatastrofičtějšího scénáře. Podle definice Evropské komise z 2. února 2000 je třeba použít princip předběžné opatrnosti vždy, "když existuje alespoň předběžný vědecký názor, že je opodstatněný důvod k obavám před riziky poškození životního prostředí či zdraví lidí, živočichů a rostlin, která by mohla narušit základní princip vysoké úrovně ochrany životního prostředí."

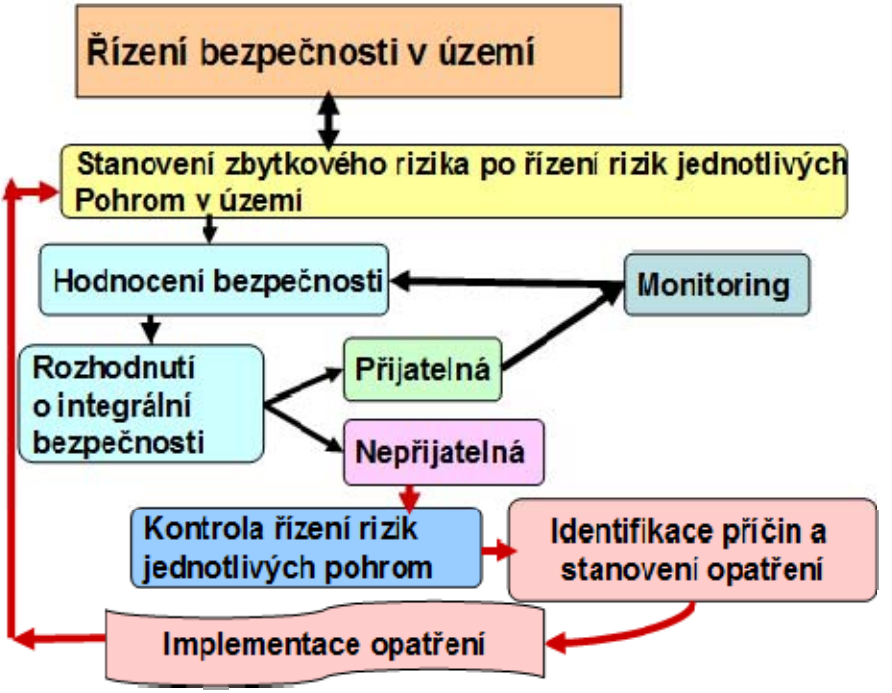
Řízení bezpečnosti spočívá v plánování, organizování, přidělování pracovních úkolů a v kontrole využívání zdrojů organizace s cílem dosáhnout požadované úrovně bezpečnosti. Zvýšení bezpečnosti se dosáhne využíváním (aplikací, realizací, implementací) technických, právních, organizačních, vzdělávacích aj. ochranných opatření. Řízení bezpečnosti se někdy označuje jako řízení rizik ve prospěch bezpečí, do kterého se zahrnuje i udržitelný rozvoj. Je běžné při plánování, projektování, výstavbě a provozu technických zařízení a objektů, jakými jsou elektrárny, přehrady, jaderná zařízení aj. (je základem jaderné bezpečnosti, radiační ochrany a ochrany před nebezpečnými chemickými látkami, zaváděné direktivou Seveso II). V technickém slangu říkáme, že v jeho rámci se zohledňují tzv. nadprojektové havárie. Řízením bezpečnosti se vytváří inherentní bezpečnost lidského systému vůči projektovým pohromám a implementací principu předběžné opatrnosti zajišťuje zvýšení odolnosti vůči nepřijatelným dopadům nadprojektových pohrom, jejichž výskyt je tak málo pravděpodobný, že je nepředvídatelný.

Každá entita se skládá z řídicího systému a z řízených systémů. Na základě současného poznání řídicí systém entity je systém pro strategické řízení bezpečnosti entity, protože právě on zajišťuje potřeby lidí a lidské společnosti [1,9]. Úkolem řízení bezpečnosti entity je zajistit žádoucí bezpečnostní situaci, tj. růst úrovně bezpečnosti a udržitelný rozvoj s ohledem na chráněná aktiva. Proto systém řízení bezpečnosti obsahuje řadu sektorů (na úrovni státu technický, vojenský, legislativní, finanční, ekonomický, sociální, ekologický, vzdělávací, výzkumný apod.). Schéma rozhodování o bezpečnosti, které se do praxe zavádí od konce 80. let, je na obrázku 2. Protože bezpečnost je v čase proměnná, tak se

cyklus řízení bezpečnosti spojený s cyklem hodnocení bezpečnosti musí v čase opakovat. Prosazování kultury bezpečnosti (tj. jednání všech lidí zaměřené na zvyšování integrální bezpečnosti) v praxi vyžaduje jak cílené řízení, tak i širokou účast státních orgánů, právnických a podnikajících fyzických osob, i občanů, vede pochopitelně k přiřazení vyšší priority plánování a řízení bezpečnosti a také k pochopení potřeby bezpečnosti všemi účastníky [9].

Pro zajištění bezpečného prostoru, ve kterém se nachází entity, je nutné zejména:

- zvyšovat informovanost o očekávaných rizicích územních celků, koncepcích, ochraně, opatřeních a postupech ke zvládnutí rizik a také o těch, která je ještě třeba přijmout a implementovat,
- zvyšovat důvěru občanů v to, že veřejná správa má skutečně cíl zajistit pro ně bezpečný prostor,
- vytvářet vzdělávací systém, který úředníkům, zaměstnancům právnických a podnikajících fyzických osob i občanům umožní porozumět bezpečnostním otázkám,
- prosazovat spolupráci a koordinaci úkolů a vzájemné sdílení informací.



Obr. 2
Schéma rozhodování o bezpečnosti entity

Položky, které je třeba sledovat při řízení bezpečnosti

Každá entita je z odborného pohledu systémem systémů [3], a proto pro podporu úspěšného řízení rizik ve prospěch bezpečí a udržitelného rozvoje potřebuje:

1. Popis a charakteristiku systému, který má více chráněných aktiv chápaných systémově a mezi nimi existují různé vnitřní vazby a toky.
2. Odolnost, zranitelnost a adaptabilitu jednotlivých systémů i systému systémů. Potřebuje znát, kdy (při jaké kombinaci vlastností) je systém udržitelný, jaká je jeho kritičnost apod.
3. Určení integrálního rizika (v systému je více chráněných aktiv, 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. Legislativu pro podporu řízení bezpečnosti systému systémů.
9. Kontrolní mechanismy pro monitorování (úrovně) bezpečnosti systému systémů.

Abychom zajistili stanovené cíle, tj. bezpečí a udržitelný rozvoj entity, je třeba, aby se bezpečnost zvyšovala. Předmětný požadavek lze obecně zajistit různými mechanismy řízení bezpečnosti (tj. různými zacílenými systémy řízení bezpečnosti – SMS či jinými slovy různými programy na zvyšování bezpečnosti), které sestavíme způsobem používaným ve strategickém řízení, tj.:

1. Formulace MISE (stanovení záměru, tj. hlavního smyslu zpracování dlouhodobého plánu rozvoje bezpečné entity jako prostředku, který zajistí bezpečnou entitu s potenciálem udržitelného rozvoje, a to dnes i v budoucnosti s tím, že jsou zváženy možné změny v čase i území).
2. Zpracování PROFILU entity (vytvoření verifikovaného datového souboru o entitě s určitou vypovídací hodnotou, který bude podkladem pro vnitřní a vnější analýzu podmínek a možností dané entity s ohledem na stanovený záměr).
3. Provedení SWOT ANALÝZY (zhodnocení parametrů entity, vlastních předpokladů řídícího týmu a ostatních zúčastněných a vnějších faktorů, které působí na entitu a jsou důležité pro její rozvoj).
4. Vymezení STRATEGICKÝCH OBLASTÍ (tj. oblastí, které mají klíčový význam pro rozvoj bezpečné entity i stanovený záměr).
5. Formulace VIZE (žádoucího cílového stavu entity, tj. společně sdílené představy o tom, jak má entita v budoucnosti ve vymezených klíčových oblastech vypadat).
6. Stanovení STRATEGICKÝCH ZÁMĚRŮ (tj. klíčových požadovaných tendencí vývoje území v jednotlivých klíčových oblastech, zhodnocení důležitosti jednotlivých záměrů a popis jejich vzájemných vztahů).

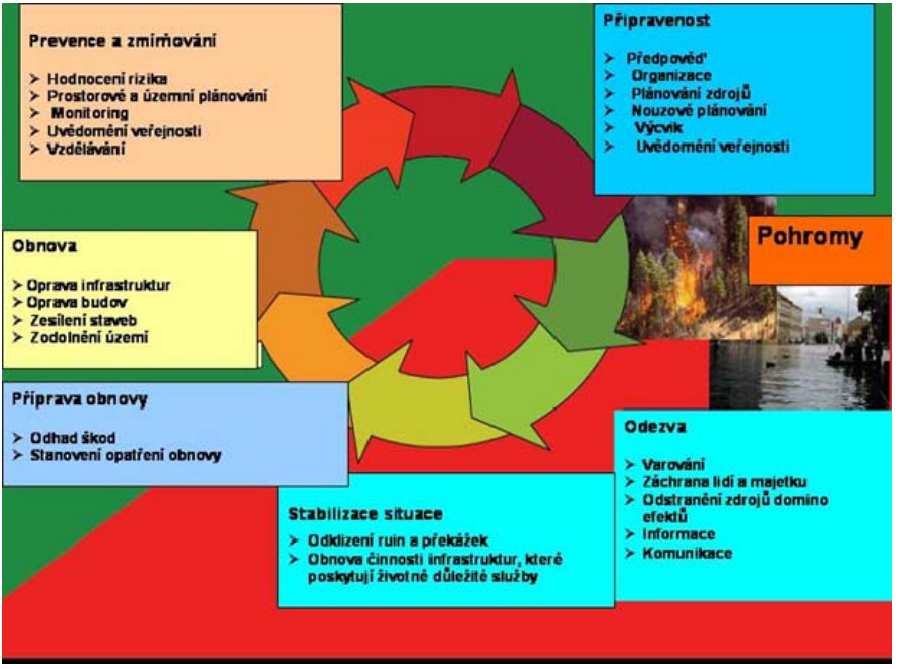
7. Zpracování IMPLEMENTAČNÍCH PLÁNŮ (stanovení konkrétních dílčích cílů pro realizaci jednotlivých strategických záměrů a z nich vyplývajících úkolů, stanovení priorit cílů a úkolů, plán realizace úkolů zahrnující termíny zahájení a ukončení, odpovědnosti a podmínky nutné pro jejich splnění).
8. Založení MONITORINGU (vytvoření systému sledování a vyhodnocování průběhu a výsledků realizace dlouhodobého plánu rozvoje bezpečné entity včetně aplikace korekčních opatření).
9. REALIZACE implementačních plánů (provádění praktických opatření ke splnění konkrétních cílů).
10. MONITORING (sledování a vyhodnocování průběhu realizace dlouhodobého plánu rozvoje bezpečné entity včetně určení aplikace příslušných korekčních opatření).
11. ADAPTACE (úprava dlouhodobého plánu rozvoje bezpečné entity v závislosti na průběhu a výsledcích realizace, na vývoji situace uvnitř i vně dané entity).
12. Na základě současného poznání je řízení bezpečnosti systému disciplína, která aplikuje metody, nástroje a techniky založené na inženýrských a manažerských přístupech tak, aby systém byl bezpečný. Opírá se o řízení rizik, ve kterém je zapracován princip předběžné opatrnosti. V případě komplexního řízení bezpečnosti jde o řízení komplexního (integrálního) rizika. Komplexní (integrální) řízení bezpečnosti je pak disciplína pro řízení bezpečnosti SoS (systému systémů). Při vytváření nových systémů nám jde o to, aby systém byl bezpečný během celého svého životního cyklu a aby neohrožoval okolní systémy. Zajištění takto chápané bezpečnosti se z hlediska řízení rizik vyznačuje zejména následujícími znaky: umísťování – projektování – konstrukce – návrh s minimalizací rizik; provozování se začleněním systému včasného varování a procedur pro řízení přijatelné úrovně rizik; a zvládnutí abnormálních, nouzových a kritických stavů při provozu i odstavení.

Z metodického pohledu řízení integrální bezpečnosti systému (lidského systému, území, životního prostředí, lidské společnosti, kritické infrastruktury atd.) představuje koordinaci řady nesourodých procesů, které probíhají současně v různých oblastech a některé jejich výsledky se vzájemně podmiňují, tj. procesy jsou jistým způsobem na sobě závislé, tj. zvládnutí příslušných úkolů je určováno usměrněním k danému cíli. Z pohledu daného cíle je nutné, aby každý jeho účastník chápal každý problém v existujících souvislostech a hledal jeho efektivní řešení v daných podmínkách, přitom postupoval racionálně a s ohledem na náklady a dostupné zdroje v příslušných oblastech. Proto všechny výše uvedené aspekty musí být zohledněny ve scénáři řízení bezpečnosti. Naplnění je možné jen tehdy, když je k dispozici kvalitní nástroj pro sestavení scénáře na řízení bezpečnosti, který je: dostatečně flexibilní; transparentní; přesný ve smyslu, že zajišťuje při opakování stejné výsledky; a správný ve smyslu, že u výsledků jsou oceněné jak nejistoty, tak neurčitosti. Pro vytvoření nástroje na sestavení scénáře řízení bezpečnosti území se používají současné poznatky a zkušenosti z řízení pohrom a z teorie řízení proměnných systémů. V praxi je však řada problémů, které jsou

nestrukturované a u řady prvků, vazeb i toků posuzovaného systému jsou nejen nejistoty, ale i neurčitosti. Pro získání schopnosti uvedené problémy řešit dávají na základě současných znalostí východisko jen metodika aplikace případové studie při rozhodování v systémovém pojetí a expertní metody.

Základní fáze řízení bezpečnosti

Každé řízení určitého úseku zahrnuje čtyři základní fáze: prevence pohrom, připravenost a odezva na vzniklé nouzové situace a obnova po pohromách [1], obrázek 3. Prevence a obnova se soustřeďují na zajištění odolnosti vůči pohromám; připravenost a odezva se soustřeďují na zvládnutí (zdolání) vyvolaných nouzových situací. Je skutečností, že řada opatření a činností odezvy, při které jde o snížení újmy a škody na chráněných aktivech, a to především na lidských životech a zdraví, majetku a životním prostředí za přijatelných nákladů, zdrojů, sil a prostředků, vyžaduje rychlé provedení a je podobná až stejná pro řadu nouzových situací. Např. záchranné a likvidační práce po povodni či požáru či vichru či technologické havárii apod. jsou stejné – jde o záchranu životů a zdraví lidí, majetku a životního prostředí a o stabilizaci situace v postižené oblasti.



Obr. 3
Časová posloupnost fází řízení bezpečnosti

V dnešní společnosti, která je závislá na dobré funkci řady technologií a infrastruktur, je často při odezvě na nouzové situace většího rozsahu nutno provést nejprve činnosti podporující provoz infrastruktur a technologií (např. dodávka elektrického proudu, vody, zajištění dopravní dostupnosti, zvládnutí paniky a chaosu apod.) k zajištění zázemí pro provádění klasických záchranných a likvidačních prací v potřebném rozsahu. To znamená, že odezva má daleko širší rozsah, než je jen zásah určitých bezpečnostních složek nebo jejich systémového propojení. Pro jakoukoliv odezvu platí, že každá časová prodleva zvyšuje ztráty a škody. Kvůli zvýšení účinnosti a efektivity odezvy je nutné, aby systémy odezvy nižších a širších celků byly provázané, tj. aby systémovým řízením byly odstraněny zdroje možných konfliktů ve všech důležitých sférách, tj. minimálně ve sféře řízení, technické, finanční, právní, personální, znalostní apod.

Nouzové plánování

Řízení bezpečnosti jako kvalifikované a uvědomělé řízení se opírá o kvalifikované plánování a zahrnuje v nejobecnějším pojetí vedení, správu, ovládání a úřední projednávání. Plánování představuje uvědomělou činnost lidí směřující k nastavení, určování a kontrole průběhu procesů pro dosažení určených cílů. Uvádí do souladu jednotlivé činnosti a plní všeobecné funkce entity, tj. jedná se o činnost, při které se vytváří podklady pro rozhodování v současné době i v budoucnosti. Proto je důležitý popis a pochopení jak problému, tak situace, v jaké se problém řeší nebo bude řešit a představa o možných změnách v území i v čase. Plánování se skládá z následujících činností: popis a prognóza možných situací a změn v území; monitorování stavu a změn v území; a návrh a příprava odezvy na změny (nápravná opatření) v případech, že vývoj nebude probíhat dle předpokladů.

Uvědomělá činnost řídících subjektů entity spočívá ve volbě a předpokládání cílů, úkolů, variant a způsobů, které podmiňují dosažení daných cílů. Za nejdůležitější rys plánování se považuje volba cíle. Plánování není sestavení hierarchického souboru příkazů, které se mají bezmyšlenkovitě plnit, představuje tvůrčí činnost, která stanovuje reálný cíl a určuje nejvýhodnější způsob jeho dosažení. V praxi se při řízení bezpečnosti setkáváme hlavně s plány: bezpečnostními, nouzovými (jejich specifické druhy jsou plány havarijní a povodňové), krizovými, kontinuity a obnovy. Plánování je spolehlivé, když: postupy jsou formalizované; obsahují opatření k omezení (zmírnění) dopadů; jde o kontinuální proces; umožní zvládnout nouzové situace; jsou multidisciplinární (tj. nejsou naivní a levné); existují postupy, jak využít připravených zdrojů; a existují postupy, jak využít bezpečnostní infrastrukturu.

Celosvětově je ověřeno [1,4,7], že vážné kritické situace vyvolá jen málo pohrom (cca 1 %), jestliže se provádí tzv. nouzové plánování, tj. plánování, jehož cílem je zvládnout všechny nouzové situace, které mohou vyvolat možné pohromy pomocí standardních prostředků, výkonných složek a financí. Všeobecným cílem nouzového plánování je ochrana lidského systému. Konkrétní cíle nouzového plánování jsou:

- realizovat preventivní opatření s cílem zabránit výskytu pohrom nebo zmírnit dopady pohrom,
- zajistit přípravu různých plánů odezvy pro různé druhy očekávaných pohrom,
- zajistit ochranu obyvatelstva a majetku při nouzových situacích,
- zajistit nezbytné monitoringy, tj. sběr, zpracování a interpretaci dat, která jsou důležitá pro ochranu obyvatelstva při očekávaných nouzových situacích,
- zajistit kontrolu bezpečnosti průmyslových podniků a přeprav rizikových materiálů,
- organizovat databázi o nouzových situacích a výcvik expertů,
- řídit státní inspekce a provádět státní kontroly s cílem odstranit nebo zmírnit nouzové situace,
- zajistit provádění výcviku v oblasti prevence vzniku nouzových situací, připravenosti a zásahu,
- zajistit efektivní odezvu na nouzové situace a minimalizovat jejich dopady na populaci a životní prostředí,
- zajistit po zvládnutí nouzové situace obnovu všech základních služeb zaručujících bezpečné přežití lidí,
- vybudovat organizaci včasného varování a zajistit informovanost obyvatelstva v době nouzové situace nebo je-li to možné i před jejím vznikem,
- ustanovit, vycvičit, naplánovat a udržovat přijatelnou úroveň připravenosti výkonných složek a řídících orgánů, které realizují nouzové plánování a provádí zásahy,
- zajistit koordinaci výkonných složek provádějících zásah,
- provádět výcvik občanů v sebeochraně a ve vzájemné výpomoci,
- zajistit informovanost obyvatel o nutných akcích při nouzových situacích,
- vytvářet a realizovat právní a ekonomická pravidla na ochranu populace a území při nouzových situacích,
- realizovat vědecké a technické programy s cílem zajistit předcházení nouzovým situacím,
- provádět humanitární činnosti,
- realizovat opatření pro sociální ochranu obětí nouzových situací,
- mezinárodně spolupracovat v oblasti ochrany obyvatelstva a území při nouzových situacích.

V České republice se nouzové plánování soustřeďuje pouze na povodně a na havárie s přítomností nebezpečných látek. V oblasti krizového plánování, které navazuje na nouzové plánování a kromě standardních zdrojů, sil a prostředků používá také nadstandardní, tj. stanovené rezervy, opatření a činnosti, jejichž použití je vázané na vyhlášení krizového stavu; je k dispozici 23 typových plánů, které z odborného hlediska představují obecné scénáře odezvy; tj. nejsou v nich zohledněna místní specifika jako v konkrétních plánech sestavených pro určitou entitu.

Plány musí mít hierarchickou strukturu, protože hierarchické jsou jak procesy, tak zdroje. Nejčastěji se používají tři úrovně, a to: 1 – důkladná analýza rizik stanovuje strategická pravidla: základní klasifikace klíčových procesů a zdrojů a jejich zabezpečení; a plán zachování funkčnosti. 2 – zajištění dat a

informací pro rozhodnutí o aplikaci připravených opatření a činností. 3 – seznam konkrétních realizačních opatření. Žádný plán entity nesmí být pouhou papírovou iluzí a musí vycházet ze znalostí o chování entity a jejich aktiv. Je třeba plánovat spíše to, co ***asi*** se bude odehrávat než to, co ***by se mělo*** odehrávat s ohledem na vztahy mezi aktivy a entitami. Každý plán musí být svázán se zdroji a měl by být znám všem zúčastněným a jimi přijímán. Plánování začíná výběrem obecně platných kritérií rozhodování a cíli, které se musí nebo chtějí dosáhnout. Každý racionální plán spojený s řízením bezpečnosti identifikuje problémy a příležitosti a hledá alternativy a způsoby jednání. Zvolené činnosti musí mít znaky efektivnosti (správné činnosti) a účinnosti (poměr vstupního úsilí a výsledků). V praxi je třeba zajistit, aby soustava plánů na sebe navazovala [1].

SWOT analýza je metoda vhodná pro strategické plánování bezpečnosti entity, když zvážíme požadavky spojené s bezpečím a udržitelným rozvojem entity [1]. Pro počáteční identifikaci rizik je vhodná metoda What, If, pro hodnocení pak metody splňující podmínky transferu technologií založené na vhodných procesních modelech procesů v entitě (lineární, stromový, síťový) a u nestrukturovaných problémů na optimalizačních metodách založených na variantách zjištěných např. metodou případové studie a na multikriteriálním hodnocení možných variant řešení; pro posouzení kritičnosti procesů a pro určení problémů, které je třeba v zájmu entity a jejich chráněných aktiv řešit, se používá matice kritičnosti apod. [8].

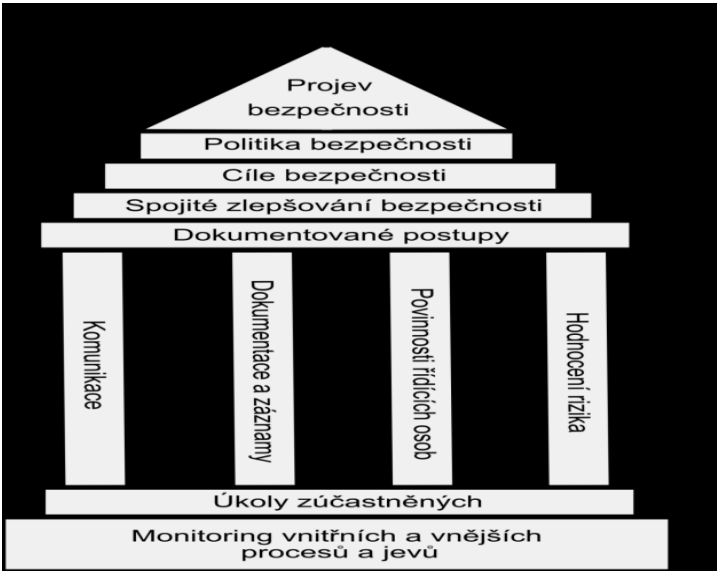
MODEL SYSTÉMU ŘÍZENÍ BEZPEČNOSTI

Strategie pro zajištění bezpečí a udržitelného rozvoje každé entity [1,4,5] spočívá v: aplikaci systémového a pro-aktivního řízení, které se opírá o znalosti a zkušenosti získané pro entitu z kvalifikovaných dat; aplikaci kvalifikovaného vyjednávání s riziky ve prospěch bezpečí a udržitelného rozvoje entity; vypořádání rizik pomocí prevence, zmírnění, pojištění, rezervy, připravenosti na odezvu a obnovu a sestavení plánu na zvládnutí nepředvídaných situací; aplikaci správného řízení, ve kterém jsou provázané řízení bezpečnosti, nouzové řízení a krizové řízení; sestavení programu na zvyšování bezpečnosti v entitě; stanovení měr na posuzování úrovně bezpečnosti ve smyslu účinnosti bezpečnostního systému (indikátory); naplnění programu provázanými projekty + naplnění projektů provázanými procesy; aplikaci adresného přidělení úkolů a odpovědností všem zúčastněným; a realizaci, která je spojená s kvalifikovaným a důsledným monitoringem. Základním principem je: kvalifikované propojení řízení oblastí technické, organizační, finanční, personální, sociální, znalostní; jasné role a odpovědnosti všech zúčastněných. Systém řízení bezpečnosti na úrovni státu (SMS – Safety Management System) proto zahrnuje řadu oblastí, tj. technickou, vojenskou, legislativní, finanční, ekonomickou, sociální, ekologickou, vzdělávací, výzkumnou apod. Úkoly jednotlivých zúčastněných a jejich propojení v různých situacích stanoví právní předpisy, morální a jiné standardy a normy.

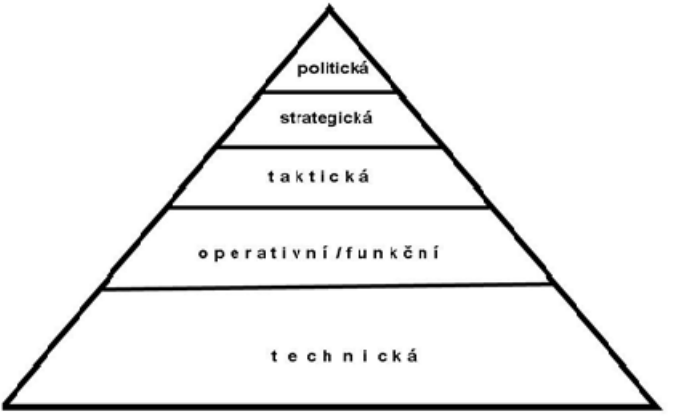
Na základě současného poznání [2] byl sestaven přehledný model systému řízení bezpečnosti (SMS), obrázek 4. Je si třeba uvědomit, že uvedený model SMS

platí pro systémy s nepříliš složitou strukturou a s jasně definovanými vztahy a toky mezi elementy systému. I zde však platí, že vzhledem k rozmanitosti systémů, které jsou objektem řízení, je nutné každý konkrétní SMS rozpracovat podle konceptu, který respektuje konkrétní strukturu a specifika systému, jímž nahrazujeme entitu, kterou chceme řídit. Uvedeným konceptem určujeme též, jaká rizika sledujeme a jakým způsobem je zvažujeme, tj. zda rozhodování při řízení provádíme podle výsledků hodnocení rizik dílčích, integrovaných nebo integrálních. Je třeba zdůraznit, že pouze integrální rizika zahrnují průřezová rizika, která jsou spojená s vnitřními závislostmi mezi vzájemně propojenými aktivy systémů nebo mezi vzájemně propojenými jednotlivými systémy v případě tzv. systémů systémů (SoS – System of Systems).

V případě reálných entit je třeba řešit konflikty mezi jednotlivými entitami. Řešení konfliktů s cílem zajistit bezpečnost SoS v reálném prostředí znamená hledání konsensu mezi cíli řízení bezpečnosti dílčích systémů a mezi způsoby jejich dosahování; prioritní cíl pro bezpečnost SoS je koexistence dílčích systémů [10]. Největším problémem systémů pro řízení bezpečnosti SoS je identifikace, pochopení a vhodné řízení průřezových rizik, která působí nebo mohou způsobit různé kaskády selhání funkčnosti SoS, které poškozují aktiva SoS. Z obecného pohledu dopady průřezových rizik (jejichž původci jsou nežádané vnitřní závislosti (interdependences) nebo závislosti mezi systémem a okolím, nejsou pouze kaskády nežádoucích jevů), ale i projevy synergie, umocnění, urychlení a hlavně dominové efekty. Úrovně řízení používané v teorii a praxi jsou znázorněny na obrázku 5.



Obr. 4
Obecný model systému řízení bezpečnosti reálných entit



Obr. 5
Úrovně řízení používané v teorii a praxi řízení

POUŽÍVANÉ KONCEPTY MANAGEMENTU A INŽENÝRSTVÍ

Inženýrství je široká disciplína, která řeší problémy od jejich pochopení, přes návrh řešení až po realizaci v daných podmínkách. Je hnací silou lidského vývoje, protože se zabývá i problémy, které je obtížné přesně řešit. K dosažení cíle používá kreativitu lidských jedinců a přístupy označované jako dobrá praxe [2]. Inženýrské disciplíny zaměřené na bezpečnost převádí cíle řízení bezpečnosti do praxe na úrovni základní, tj. technické, a proto mají zásadní důležitost. V inženýrských disciplínách platí, že cílem řízení systému prostřednictvím řízení rizik nebo vyššího typu řízení, tj. řízení bezpečnosti, je zabránit, aby se systém nedostal do nežádoucích, tj. nepřijatelných stavů a uspořádání. K tomu je však nezbytné vědět, ve kterých aspektech systému „sídlí“ zranitelnost a pružná odolnost (houževnatost). Přitom se vychází z dále uvedených předpokladů:

1. Systém obsahuje vnitřní prahové hodnoty a má procesy, které produkují prahové hodnoty.
2. Rozložení pravděpodobnosti pro klíčová rozhodnutí je vysoce neurčité (proto je nutné se vyhýbat pravděpodobnosti, pokud není „podpořena“ daty).

Subjekt, který rozhoduje o systému, rozhoduje na základě neúplných znalostí o klíčových zdrojích.

Historický vývoj manažerských a inženýrských disciplín pracujících s riziky měl zatím čtyři kroky, které lze charakterizovat následovně:

- Předmětem řešení je jeden systém, který se považuje za uzavřený. Za zdroje rizik se berou jen jevy (pohromy), jejichž zdroje jsou uvnitř systému a při jejichž realizaci dochází k poškození systému nebo některého z jeho základních aktiv. Protože uvedenou disciplínu odstartoval rozvoj technologií, tak v samotných počátcích aktiva tvořily jen technické komponenty a jejich propojení.

- Předmětem řešení je jeden systém, který se považuje za uzavřený. Za zdroje rizik se berou jednak jevy (pohromy), jejichž zdroje jsou uvnitř systému, a jednak jevy způsobené člověkem (lidský faktor), při jejichž realizaci dochází k poškození systému nebo jeho aktiv.
- Předmětem řešení je jeden systém, který se považuje za otevřený, tj. rozlišuje se systém a jeho okolí. Za zdroje rizik se berou jednak jevy (pohromy), jejichž zdroje jsou uvnitř, a to včetně lidského faktoru, i vně systému, při jejichž realizaci dochází k poškození systému nebo jeho aktiv.
- Předmětem řešení je systém a okolí a nejnověji systém systémů, tj. komplex složený z několika propojených otevřených systémů, které plní jisté žádoucí cíle jen za určitých podmínek. Cílem je zajistit koexistenci všech systémů a bezpečnost jak jednotlivých systémů, tak celého systému systémů i okolí. Za zdroje rizik se berou jevy (pohromy), jejichž zdroje jsou uvnitř, a to včetně lidského faktoru, i vně systému, a nejnověji jevy spojené s propojeními mezi systémy a jejich okolími i jevy spojené s propojeními napříč systému systémů, při jejichž realizaci dochází k poškození systému nebo jeho aktiv.

Posledně zmíněný případ reprezentuje recentní špičkový přístup. Jeho aplikací lze např. dosáhnout konsensu mezi techniky, ekology a sociology, kteří historicky vytvořili samostatné systémy řízení pro své cíle, jejichž dosahování je často konfliktní.

Prvotní a zcela zásadní je problém, který musí být vyřešen, aby bylo získáno kvalifikované řešení určitého úkolu, který souvisí s následujícími aspekty, které musí být zváženy při stanovení konceptu řešení konkrétního úkolu spojeného s riziky. Jedná se o stanovení:

- Cíle a kontextu řešení, tj. o určení, zda problém bude řešen jako jednooborový nebo mezioborový nebo mnoha oborový a průřezový, a na jaké odborné úrovni bude řešen, tj. jako místně specifický, regionálně specifický či jako obecný. Je si třeba uvědomit, že právě zde se odlišuje pojetí řešení vědců, kteří obvykle hledají obecná řešení či parciální řešení v závislosti na souvislostech spojených s různými definicemi chování systémů a jejich okolí, a inženýrů, kterým jde o vyřešení úkolů v daných konkrétních podmínkách daných vlastnostmi konkrétního místa, legislativou včetně norem a standardů, dostupnými zdroji, a to finančními, technickými a lidskými (úroveň kvalifikace disponibilního personálu).
- Struktury předmětných systémů, tj. jejich prvků, vazeb a toků mezi prvky, které tvoří aktiva systémů, o která jde při řízení bezpečnosti systému systémů. Cíle řešení jednoho a téhož úkolu mohou být stanoveny různě, např. jde o jedno aktivum; jde o dvě či více vzájemně se podporujících aktiv; jde o dvě či více aktiv, z nichž některá se vzájemně podporují a některá jsou vzájemně konfliktní; např. kvalitní životní prostředí podporuje kvalitní život a rozvoj lidí; naopak je známa řada konfliktů mezi životním prostředím a technologiemi, mezi člověkem a technologiemi (viz specifické úseky studia jako člověk-stroj, člověk-počítač atd.).
- Kritických míst řešení úkolů na základě znalostí a zkušeností. Kromě aplikace všeobecných znalostí jde o uvědomění si příslušných zásad dobré inženýrské

praxe, protože řada úkolů z praxe nemá obecné řešení kvůli tomu, že chování systémů a jejich okolí je proměnné, proměnnost není lineární, objevují se náhlé změny apod., což znamená, že neexistuje ani dostupné analytické řešení, ani jedno určité všeobecně platné řešení.

Na základě současného chápání pojmů bezpečí a bezpečnost inženýrské disciplíny reprezentují postupy, které se používají pro umístění, plánování, návrh, výstavbu, provoz a změny činností objektů a infrastruktur v entitě a pro jejich součinnost s cílem zajistit bezpečnou entitu a bezpečnou lidskou společnost, které znamenají bezpečný lidský systém.

ZÁVĚR

Bezpečnost každé entity závisí na procesech, dějích a jevech, které probíhají v dané entitě a v jejím okolí. Nelze ji jednoduše kvantifikovat, a proto se hledají její míry i míry jejího trendu v čase. Z pohledu bezpečí a udržitelného rozvoje entity je podstatné, zda:

- úroveň bezpečnosti v čase roste či klesá,
- ve stanovených časových úsecích je dosahováno plánované úrovně bezpečnosti,
- aplikovaná opatření vedou skutečně ke zvýšení úrovně bezpečnosti.

Pojetí integrální bezpečnosti systému vytvořené pro entitu dovoluje:

- uvědomit si aspekty systému, které jsou důležité pro jeho bezpečí a udržitelný rozvoj,
- pochopit příčiny poruch v chování systému a kontext jejich působení,
- soustředit pozornost na podobnosti i rozdíly pohrom samotných,
- pochopit roli entity ve spojitosti s bezpečností, tj. především vlastnosti entity, které eskalují nebo potlačují dopady pohrom vždy nebo jen za určitých okolností,
- používat uvědoměle metodiky hodnocení pohrom, jejich dopadů i identifikace nápravných opatření,
- stanovit cíle, harmonogramy, monitoringy, organizační struktury, normy, standardy a právní předpisy pro uvědomělé řízení bezpečnosti systému,
- odstranit multiplicity při přípravě opatření na zvládnutí dopadů pohrom,
- při územním plánování, projektování, výstavbě, provozování, odezvě na pohromu v entitě a při obnově entity neaplikovat opatření, která zvyšují rizika spojená s dalšími možnými pohromami v dané entitě.

Pro potřeby řízení bezpečnosti entity se zajišťuje sledování systému z pohledu celku i z pohledu jednotlivých komponent systému, tj. prvků či subsystémů, vazeb a toků.

Résumé

The paper deals with the integral safety of human system and on its management in the profit of security and sustainable development of humans. It

starts with the introduction into problems of integral safety and its management. With regard to fact that level of safety depends on quality of tools for trade-off with risks, it specifies problems domains and it determines the strategy for management faced to ensuring the targets. It gives: data on assets´ vulnerability (i.e. dependence of asset damages on disaster severity), safety management phases and principles, i.e. principles of management of risks in the benefit of security and sustainable development of humans and the other assets that human essentially needs for life; general model of safety management system or real entities (SMS); and levels of problems solving used in theory and practice of management.

Literatura

[1] PROCHÁZKOVÁ, Dana. *Strategické řízení bezpečnosti území a organizace*. Praha: ČVUT, 2011. 483 s. ISBN 978-80-01-04844-3.

[2] PROCHÁZKOVÁ, Dana. *Bezpečnost kritické infrastruktury*. Praha: ČVUT, 2012. 318 s. ISBN 978-80-01-05103-0.

[3] PROCHÁZKOVÁ, Dana. *Analýza a řízení rizik*. Praha: ČVUT, 2011. 405 s. ISBN 978-80-01-04841-2.

[4] HAYS, Walter, ed. *Global Blueprints for Change – Summaries of the Recommendations for Theme A „Living with the Potential for Natural and Environmental Disasters“,Summaries of the Recommendations for Theme B „Building to Withstand the Disaster Agents of Natural and Environmental Hazards“,Summaries of the Recommendations for Theme C „Learning from and Sharing the Knowledge Gained from Natural and Environmental Disasters*. Washington: ASCE, 2001.

[5] ARMSTRONG, Marcus. *Management Processes and Functions*. London: CIPD, 1996. ISBN 0-85292-438-0.

[6] PROCHÁZKOVÁ, Dana et al. FOCUS project study. FOCUS website. Dostupné z: http:// www.focusproject.eu/documents/14976/-5d763378-1198-4dc9-86ff-c46959712f8a

[7] OCHA: *OCHA Orientation Handbook on Complex Emergencies*. Geneve: OCHA, 2000.

[8] PROCHÁZKOVÁ, Dana. *Metody, nástroje a techniky pro rizikové inženýrství*. Praha: ČVUT, 2011. 369 s. ISBN: 978-80-01-04842-9.

[9] OECD: *Guidance on Safety Performance Indicators. Guidance for Industry, Public Authorities and Communities for developing SPI Programmes related to Chemical Accident Prevention, Preparedness and Response*. Paris: OECD, 2002. 191 s.

[10] BOSSEL, Hans. *Systeme, Dynamik, Simulation – Modellbildung, Analyse und Simulation komplexer Systeme*. Books on Demand, Norderstedt/Germany, 2004. ISBN 3-8334-0984-3. Dostupné z: www.libri.de