Integrovaná bezpečnosť / Integral safety 2015
Proceedings of the International Scientific Conference, Rajec, September 18, 2015. - Slovak Society for Environment /Strix: Žilina, Edition ESE-22, First Edition, ISBN 978-80-89753-04-8 ▪ Rusko, M. [Ed.] ▪

BEZPEČNOST JE INTERDISCIPLINÁRNÍ A MNOHO DISCIPLINÁRNÍ OBOR

Dana PROCHÁZKOVÁ

SAFETY IS INTERDISCIPLINARY AND MULTIDISCIPLINARY DISCIPLINE

Abstrakt
Článek dokládá, že bezpečnost a řízení bezpečnosti jsou mezioborové a mnohaoborové disciplíny. S ohledem na předmětnou skutečnost projekty zabývající se řešením jejich problémů nelze kvalifikovaně zatřídit do systému oborů, který je v platném českém číselníku vědeckých oborů, který používají agentury, které rozdělují peníze na projekty.

Klíčová slova: *Bezpečí. Bezpečnost. Řízení bezpečnosti. Inženýrství bezpečnosti. Mezioborová a mnoha oborová vědní disciplína*

Abstract
The paper documents that safety and safety management are interdisciplinary and multidisciplinary fields. With regard to mentioned reality the projects dealing with solution of their problems may not be well included into the system of fields that is in valid Czech list of scientific fields that used the agencies that divide finances on projects.

Key words: *Security. Safety. Safety Management. Safety Engineering. Interdisciplinary and Multidisciplinary Scientific Field*

1. Úvod do problematiky

Při diskusi s některými dnešními odborníky lze získat různé informace. Jejich kvalita se v řadě případů neodvíjí od všeobecného poznání a od letitých zkušeností, které patří do znalostní databáze lidstva, ale od jejich vlastních představ, které si vybudovali na základě představy o prioritě jejich zájmového úseku. V posledních letech jsem potkala několik specialistů, kteří mne svými názory donutili napsat veřejné zdůvodnění o zařazení problematiky bezpečnosti a problematiky řízení bezpečnosti. Ač v osmdesátých letech minulého století byla řada disertací s mnohaoborovou a mezioborovou tématikou, tak do dnešního dne v seznamu oborů na státní úrovni chybí obory pokrývající zmíněnou tématiku.
V důsledku uvedené skutečnosti dochází ke kuriózním situacím, ve kterých např. při zadávání projektů, technické řešení musí být zařazeno do oboru pod sociální vědy, při hodnocení projektu z oboru bezpečnosti se zástupce technických věd domnívá, že uvedená problematika se nemá řešit na technických univerzitách apod.
I když v rámci projektu Evropské unie FOCUS [1] se ukázalo, že největší brzdou pokroku je korupce a zneužití pravomoci (ve zmíněném případě hodnotitelem), tak na základě znalosti akademického prostředí si dovoluji upozornit na příliš úzkou specializovanost řady odborníků, která je ještě podporovaná představou výzkumných agentur, která je vyjádřena skutečností, že softwarový nástroj je top výsledek projektu, a proto u návrhů projektů nezkoumá kvalitu odborného zázemí software a způsob využití zkušeností z dobré inženýrské praxe, který předurčuje schopnost software řešit reálné problémy.
Výše uvedené skutečnosti jsou překvapující v době, kdy světoví odborníci ve všech oborech se orientují na vypořádání rizik a ukazují na existenci nejistot a neurčitostí při řešení problémů řízení a zvládání rizik, se kterými se je nutno dobře vypořádat, aby v praxi byly dosaženy žádoucí cíle [2-63].

2. Zacílení bezpečnosti

Na základě recentních odborných prací, standardů a norem [1-52,54,57-63], dokumentů EU [53,55,56,64] a OSN[65,66] se bezpečnost spíše zaměřuje na člověka a lidskou společnost (proto se používá pojem lidská bezpečnost), tj. ne na stát jako základní útvar organizačního uspořádání lidí. Cílem opatření a činností není jen pouhá ochrana územní suverenity, ale také bezpečí lidí a lidské společnosti, což se vzájemně nevylučuje. Tradiční pojetí bezpečnosti, používané při budování výkonných složek státu k zajištění vnitřní a vnější bezpečnosti, klade důraz na strukturované násilí. Lidská bezpečnost naproti tomu bere v úvahu dynamický systém, který se v čase mění a rozvíjí, připouští se tedy, že existují dosud nepoznané procesy, které je třeba stále poznávat a přizpůsobovat jim řízení společnosti.
V systémovém pojetí je lidská bezpečnost chápaná jako integrální bezpečnost lidského systému, která má rozměry politické, environmentální, ekonomické, technické, potravinové, zdravotní, osobnostní a komunitní, což znamená, že je vícerozměrná. Jde o vlastnost systému, na které závisí existence systému. V důsledku svého charakteru se integrální bezpečnost neomezuje jen na jednostranná řešení jako je represe, ale zabývá se situacemi ovlivňujícími určitou úroveň bezpečnosti prostřednictvím tzv. řetězce bezpečnosti, jenž se skládá z následujících částí: proaktivita (odstranění strukturálních příčin nejistoty a neurčitosti, které narušují bezpečnost); prevence (odstranění přímých příčin nejisté situace porušující stávající stav bezpečí); připravenost (řešit situaci, v níž je stav bezpečí narušen); odezva; a obnova [67].
Při zpracování dalších kapitol byla použita poznatková základna, kterou tvořila data z výše citovaných prací a z dalších prací shromážděných v práci [67], která byla analyzována, logicky srovnána na základě systémového chápání reality a

vyhodnocena s cílem vyhledat vzájemné souvislosti a konflikty. Poté byl syntézou vytvořen model splňující požadavky na bezpečí a rozvoj lidí [67] a respektující existenci několika systémů, které mají nestejné cíle a vzájemně se prolínají, tj. byly specifikovány podmínky pro jejich koexistenci [68].

3. Analýza a vyhodnocení základních poznatků

Odvěkým cílem lidí je bezpečný svět s udržitelným rozvojem. V recentních studiích svět popisujeme modelem „lidský systém“, který je v podstatě systém systémů, který je otevřený (a tím i propojený a závislý na systému planety Země a vyšších systémů, se kterými je systém planety propojen). Lidský systém se skládá z otevřených vzájemně propojených systémů, a to sociálního, environmentálního a technologického. Protože uvedené systémy mají různou podstatu i různé cíle, tak člověk, který má jistý potenciál ovlivňovat a usměrňovat chování komplexního systému, si musí uvědomovat předmětný fakt a jeho snahou musí být koexistence systémů, tj. provádění takových opatření a činností, které budou omezovat vznik konfliktů a případně i řešit vzniklé konflikty mezi zmíněnými systémy i zmíněnými chráněnými aktivy ve prospěch bezpečného lidského systému, který má potenciál rozvoje [68].
Na základě současného poznání má lidský systém několik veřejných aktiv, kterými jsou: životy, zdraví a bezpečí lidí; majetek; veřejné blaho; životní prostředí; a infrastruktury a technologie (důvody: člověk nemůže žít bez přírody, do které podstatou patří; člověk nemůže žít bez infrastruktur a technologií, které mu usnadňují život a na nichž se stal závislý). Ze systémového pojetí problematiky, cíle lidí a uvedených faktů o lidském systému a jeho aktivech vyplývají dva základní požadavky pro disciplínu, jejímž cílem je zajištění bezpečného lidského systému, a to nutnost:

- používat jisté základní pojmy: bezpečí a nebezpečí; pohroma, ohrožení a riziko; bezpečnost a nebezpečnost,
- aplikovat komplexní přístup, což znamená neřešit pouze problém zvládání dopadů pohrom, tj. nouzové situace, havárie, mimořádné události apod., ale celý řetězec úseků řízení, tj. prevenci, připravenost, odezvu a obnovu, přičemž velký důraz klást na poučení z řešení problémů odezvy a obnovy po nouzových, a hlavně po kritických situacích, které způsobují humanitární krize; tj. zajistit aplikaci strategického, systémového a pro-aktivního přístupu, založeného na celosvětovém odborném poznání i zkušenostech.

Bezpečí či nebezpečí závisí na procesech, dějích a jevech, které probíhají v lidské společnosti, životním prostředí, planetárním systému, galaxii a dalších vyšších systémech. Bezpečí je stav, ve kterém vznik újmy na člověku a dalších chráněných aktivech je málo pravděpodobný; nebezpečí je stav, ve kterém platí tvrzení opačné. Pohroma označuje všechny jevy, které od jisté velikosti působí újmu, ztráty a škody člověku a/nebo dalším chráněným aktivům. Ohrožení je normativní velikost pohromy vyjádřená v příslušných fyzikálních či jiných jednotkách daných naturelem pohromy, která určuje hranici, pro kterou platí, že člověk dělá opatření a činnosti, které zajistí, že on i veřejná chráněná aktiva jsou ochráněny před dopady pohrom s velikostí nižší nebo rovnou ohrožení. Riziko je pravděpodobná velikost nežádoucích dopadů (ztrát, škod a újmy) způsobených pohromou o velikosti ohrožení na chráněné zájmy za specifikovaný časový interval, normovaná na jednotku území a popř. na jistý počet lidí. Velikost rizika, které představuje jistá pohroma, závisí jednak na velikosti ohrožení v daném místě a jednak na množství a zranitelnosti chráněných aktiv v daném místě. Bezpečnost je soubor opatření a činností zaměřených na zajišťování bezpečí a udržitelného rozvoje člověka a dalších chráněných aktiv, tj. je to nástroj, který vyjednává s příslušnými riziky. Nebezpečnost je pak soubor všech vlastností, činností a procesů v lidském systému, které znamenají nebezpečí pro člověka a další chráněná aktiva.
Komplexní přístup znamená aplikovat strategické řízení, které je zaměřeno na dlouhodobou udržitelnost. Jeho cílem je integrita systémů, protože systémové služby podporují život podporující funkce. Považuje člověka za součást systému, integruje lidskou činnost s ochranou přírodního prostředí a reaguje citlivě na potřeby lidí v kontextu ekosystémů. V každém řídícím procesu je důležitou částí kvalitní a kvalifikované rozhodování, a proto je zapotřebí v rámci uplatňovaného systému řízení vytvořit systémy na podporu rozhodování, poněvadž rozhodování vůči systémům je složité a musí mít vícedimenzionální charakter. Vždy je třeba pracovat s vědomím, že udržitelný rozvoj se netýká jen zvyšování a udržování materiálního blahobytu, ale týká se také environmentální bdělosti, protože většina přírodních zdrojů není nekonečná (kvantita), a některé přírodní zdroje jsou také neustále kontaminovány (kvalita), což se týká zejména vody a půdy. A další dopady se dají očekávat od potenciálních změn klimatu anebo od antropogenních činností směřujících např. k nasycení téměř 7 miliard lidí. Nedostatek vody, půdy, kontaminace chemická a biologická ukazují, že problémy jsou složité v biofyzikální oblasti a kontroverzní v socioekonomické oblasti. Sledované systémy jsou složité a mnoho procesů se nedá přímo pozorovat. V socioekonomické oblasti se všechna environmentální rozhodnutí dají charakterizovat množstvím konfliktních cílů. Aby vztah mezi lidskými sídly a biofyzikálním prostředím (krajinou) byl i v budoucnu vyvážený, je třeba k řešení problémů tzv. „šedé“ (tj. lidmi vytvořené) a „zelené“ (přírodní) infrastruktury uplatňovat nový přístup, který je založený na řízení bezpečnosti v integrálním pojetí.
Protože doposud neexistuje obecná shoda na formulaci problémů udržitelnosti veřejného blaha (blahobytu) lidské společnosti v kontextu se systémovými službami, je každé dosavadní řešení dočasné, jelikož se neustále balancuje mezi konkurujícími si zájmy a společenskými cíli (jsou-li stanoveny). Je obtížné řešit problémy rozhodování jednoznačně vzhledem k měnícímu se charakteru rozhodovacího procesu. V rozhodování se řeší dále uvedená dilemata:

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

Je obtížné řešit inverzní problémy pro složitost systémů. Pakliže se stanoví a utřídí nějaké příznaky spojené s riziky, vynoří se příznaky nové. Proto praktický přístup k řízení udržitelnosti musí být iterační, interaktivní a adaptivní. Analýza vývoje životního prostředí i vývoje politické, sociální a ekonomické situace ve světě ukazuje, že je nezbytné se připravit na řešení případů a akcí, které svou intenzitou dopadů vyvolají kritické situace, což vyžaduje, aby z hlediska lidského bezpečí, rozvoje lidského systému, existence, stability a rozvoje státu a každého území byl systém řízení lidské bezpečnosti proaktivní, strategický a zahrnoval udržitelný rozvoj. V rámci tohoto moderně koncipovaného systému řízení bezpečnosti musí být nouzové řízení a uvnitř něho i krizové řízení, tj. reaktivní typy řízení, které zajistí okamžitou odezvu na situace ohrožující člověka a aktiva, která potřebuje k životu. Cílem komplexního řízení je za každé situace zajistit ochranu životů, zdraví a bezpečí lidí, majetku, životního prostředí, infrastruktury a technologií, které jsou nezbytné pro přežití lidí, tj. vždy zajistit mobilizaci a koordinaci využití národních zdrojů (energie, pracovní síly, výrobní schopnost, jídlo a zemědělství, suroviny, telekomunikace aj.), koordinaci činností takových, jako je systém vyrozumění, systém záchrany a zdravotnické služby, které snižují dopady pohrom a také kontinuitu činnosti státní správy a dodržování zákonů. Typy plánování tvořící základní metodické nástroje jednotlivých vzájemně provázaných typů řízení musí vytvářet základnu, ve které jsou výše uvedené cíle zakotvené.
Pro cíle lidské společnosti, tj. především pro její udržitelný rozvoj se musí vzájemně kombinovat opatření a činnosti na snižování zranitelnosti a na zvyšování pružné odolnosti (resilience) a schopnosti adaptace, které respektují všechny základní chráněné zájmy v jednotlivostech i celku. Podle současných znalostí a zkušeností je třeba na všech úrovních řízení implementovat proaktivní systém řízení bezpečnosti, ve kterém se upraví hodnocení rizik do takové formy, která respektuje všechna chráněná aktiva a bere v úvahu existující a prokázané vnitřní závislosti. S ohledem na současné poznání je třeba provádět a sledovat výzkum vnitřních závislostí, které zprostředkovávají sekundární a další dopady pohrom na životy, zdraví a bezpečí lidí. Uvedené skutečnosti ukazují, že projednávané záležitosti patří do všech základních vědních oborů, tj. sociálních, environmentálních i technických.

4. Jak zajistit cíle bezpečnosti

Z recentního poznání vyplývá, že bezpečnost subjektu (území, organizace, objekt, stát) závisí jednak na riziku v daném místě (tj. závisí jak na možných pohromách, které postihují dané místo, tak na místních zranitelnostech vůči jednotlivým možným pohromám, které postihují dané místo) a jednak na metodách zvládání a řízení rizik, která jsou zdrojem ztrát, škod a újmy na člověku a dalších chráněných aktivech.

Vztah mezi bezpečností a rizikem není komplementární, např. instalací varovacích systémů zvýšíme bezpečnost, ale riziko zůstane stejné.

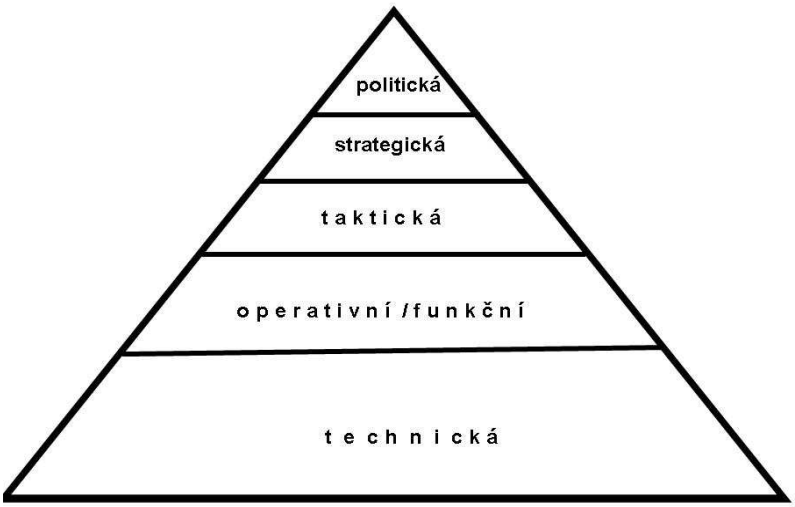
Pro potřebu řízení a zvládání rizik je třeba provést: identifikaci, analýzu, hodnocení, alokaci a ošetření rizik. Alokace rizik zahrnuje vypořádání rizik a přidělení vyjednávání s riziky jednotlivým zúčastněným. Protože svět se dynamicky vyvíjí, tak je třeba instalovat monitoring a v případě potřeby provést aplikaci nápravných opatření.
Rizika stále přibývají a lidská společnost nemá zdroje, síly a prostředky, aby tomu zabránila, a proto musí cíleně řídit rizika. Aby řízení bylo úspěšné, tak se musí zaměřit na prioritní rizika a jejich aspekty. Vyjednávání s riziky 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 státu / území / organizace; a připraví plán pro odezvu na nepředvídané situace (contingency plan) v případě rizik neřiditelných nebo příliš nákladných na eliminaci anebo málo častých.
Základním cílem státu je zajistit bezpečnost lidského systému a jeho chráněných aktiv, a proto hlavním cílem programů veřejné správy zaměřených na bezpečné území je prevence vůči pohromám a v případě přírodních pohrom, které nelze odvrátit, je to zmírnění nepřijatelných dopadů předmětných pohrom. Aby prevence pohrom a zmírnění jejich dopadů byly efektivní, je nutné, aby všichni zúčastnění na všech úrovních spolupracovali. V každém společenství je důležité, aby spolupracovali vlastníci technologií a infrastruktur, místní veřejná správa a veřejnost s cílem snížit rizika všech možných pohrom. Předmětná spolupráce musí být založena na otevřené a správné politice, která mimo jiné pomáhá také růstu důvěry lidí ve veřejnou správu i vlastníky infrastruktur a technologií v tom směru, že přijímaná opatření omezují rizika pohrom, které mají extrémní dopady.
Bezpečnost musí být proto integrální součástí podnikatelských aktivit vlastníků infrastruktur a technologií. Všechny podniky musí být řízeny tak, aby výskyt nehod, které mají vliv na bezpečnost, byl minimální. K tomu musí směřovat veškeré činnosti a úsilí řídících pracovníků i zaměstnanců. Klíčovými prvky pro daný cíl jsou vzájemná spolupráce, otevřená komunikace a pravidelné sledování plnění cílů na úseku bezpečnosti. Na základě současných požadavků zakotvených v legislativě rozvinutých zemí vlastníci technologií a infrastruktur musí pro zvyšování bezpečnosti:

- prosazovat bezpečnost jako celistvou součást svých podnikatelských činností a podporovat bezpečné činnosti,
- aktivně vyhledávat informace o bezpečnosti,
- vstupovat do spolupráce se správními úřady i s ostatními podnikateli s cílem zlepšovat bezpečnost,
- vytvářet společně s ostatními podniky podmínky pro společnou odezvu a vzájemnou pomoc,
- vytvářet profesní organizace.

Veřejná správa musí stanovovat cíle na úseku bezpečnosti, vytvářet jasný a celistvý rámec pro řízení bezpečnosti a pomocí vhodných inspekcí a vynucovacích opatření musí zajistit, že všechny relevantní požadavky na úseku bezpečnosti jsou plněny. Musí se chovat pro-aktivně při stimulaci subjektů v oblasti podpory prosazování nových přístupů v prevenci kromě své tradiční snahy zajistit zvládnutí dopadů vyskytnuvších se pohrom. Má vedoucí roli v motivaci všech sektorů společnosti pro podporu prevence pohrom a pro identifikaci nástrojů pro rozvoj národní kultury, která prosazuje prevenci pohrom. Musí rovněž zajistit, aby veřejnost dostávala včas všechny relevantní informace týkající se extrémních dopadů pohrom a aby jim porozuměla. Tím si vlastně získává důvěru veřejnosti v to, že její dozorná činnost je správná. Uvedené skutečnosti opět ukazují, že projednávané záležitosti patří do všech základních vědních oborů, tj. sociálních, environmentálních i technických.

5. Řízení bezpečnosti

Řízení bezpečnosti vychází z řízení procesů, které je založeno na důsledném využití znalostí o problému v systému a jeho okolí, a proto se mu také říká „knowledge management“. Nositelé znalostí jsou lidé, znalosti nelze nikomu odebrat, ale lze je neomezeně rozšiřovat a množit. Ve znalostní společnosti je to právě duševní kapitál, který dominuje a má zcela jiné postavení než dříve. To vše vyžaduje jiný pohled na řízení útvarů a jednotek. ***Procesní řízení založené na ovládání řídících a prováděcích procesů*** se odlišuje od operačního přístupu, který se běžně používá v rozhodovacím procesu klasického řízení. Klasické řízení je založeno na funkčním přístupu, který se zaměřuje zejména na výstupy (výsledky), což je vlastně orientace na důsledky, a ne na příčiny. Je zřejmé, že hodnocení výsledků nemusí odhalit příčiny nesplnění cíle. V okamžiku, ve kterém se zaměříme na výstupy, zanedbáváme principy prevence.
Procesní řízení založené na řízení znalostí se nezaměřuje na výsledky, ale na příčiny. Je založené na rozpracování koncepce a metodologie. Uplatnění prvků řízení znalostí v rozhodovacím procesu řídícího pracovníka vede k přechodu od individuálního rozhodování ke skupinovému přístupu. Důležitá je role řídícího pracovníka, který daný proces musí usměrňovat k přijetí kvalitního rozhodnutí. Je však třeba vzít v úvahu, že popsaný postup je nejenom časově náročnější, ale je také náročnější na přípravu jednotlivých členů procesního týmu včetně řídícího pracovníka. Ze zkušeností při uplatňování prvků procesního řízení v podnikové sféře vyplynulo, že při rozhodování rutinním je individuální rozhodnutí výhodnější, pro přípravu rozhodnutí neprogramového (tj. složitého a nestandardního) je žádoucí volit metodu skupinového rozhodování (vytvoření procesního týmu). V obou případech však je řídící pracovník vždy za rozhodnutí odpovědný. Při skupinovém rozhodování musí být také vytvořeno vhodné prostředí, které bude podporovat tvůrčí schopnosti skupiny. Je důležité, aby řídící pracovník uměl potlačit vliv neschopných, neznalých a líných, ale ambiciózních jedinců, kteří pro prosazení svých ambicí útočí na znalé a pracovité. Řídící pracovník musí při týmovém rozhodování zajistit: podporování původnosti a neobvyklosti řešení, které je nadčasové; řízení skupiny tak, aby byly odděleny zdroje od obsahu informací; zabezpečení uplatnění nezávislého osobního úsudku a zkušeností; udržování otevřené komunikace, posilování sebedůvěry, zabránění zesměšňování; zabránění rychlých řešení a krátkodobých výsledků; a dosažení konsenzu. Pokud to není možné, přijmout a implementovat rozhodnutí po důsledném vyhodnocení všech okolností, které mohou mít vliv na dosažení cíle.
Rozlišujeme základní úrovně řízení, které je nutné sladit, a to: politická, strategická, taktická, operativní / funkční a technická, obrázek 1. Politická úroveň je často ovlivněna představami a mocenskými cíli vládnoucích politických reprezentací, a tím je někdy vzdálena od cílů, které má řízení procesů založené na znalostech. Je však důležitá, protože jejím prostřednictvím se realizují ostatní úrovně. Je výrazně ovlivněna jevy, jako jsou: korupce, mocenské vztahy, zneužití pravomoci a lobbyismus.



Obr. 1. Úrovně řízení procesů

V procesním řízení založeném na znalostech strategická úroveň určuje základní směry vývoje, ze kterých vyplývá, které procesy je nezbytné upravit nebo vytvořit, jaké organizační změny bude nezbytné provést, kde získat know-how, finanční

zdroje atd. Taktická úroveň řízení procesů pomáhá utřídit činnosti nutné pro realizaci dlouhodobých záměrů. Hledají se odpovědi na otázky jak procesy nastavit, v jakém stavu je udržovat a jak musejí tyto procesy navzájem spolupracovat. Operativní řízení rozhoduje o konkrétním rozmístění zdrojů v procesu (lidských, technologických, finančních) a také o výkonu jednotlivých činností v rámci nastavených procesů (jak provést konkrétní operaci). Snahou je zajistit transfer znalostí a dovedností mezi pracovníky. Na technické úrovni se řeší konkrétní problémy. Je si třeba uvědomit, že nejnáročnější je vyjednávání s riziky, které se odehrává právě na této úrovni; zvyšuje se odolnost prvků, zařízení, komponent i celých systémů a dle údajů z praxe úspěšnost technických opatření se pohybuje mezi 40 a 80%. Významného efektu a ***konkurenční výhody subjekt*** (území, organizace) ***dosáhne teprve sladěním všech úrovní řízení.*** Cílem je dosáhnout stavu, kdy procesy jsou definovány a řízeny na základě strategie, operativní řízení není jen hašením mimořádných událostí, ale je zacílené na úspěšné plnění rozvojových cílů. Procesy jsou zdokonalovány na základě poznatků přenášených z operativy. Nové poznatky pramenící z řízení procesů se pak rychle promítnou zpět do strategie a vyvolají další zásadní změny ve vývoji subjektu.
Procesní řízení je založeno na principu integrace činností do ucelených procesů, tj. dílčí operace se sjednocují do procesů. Procesy jsou ovládané procesními týmy. Každý procesní tým řídí procesy na svém stupni a podřízeným skupinám dává úkoly, které vedou k naplnění cíle. Přitom všechny procesní týmy jsou motivovány k dosažení optimálních výsledků a všechny stupně sledují při dosahování dílčích výsledků splnění konečného cíle. V procesním řízení existují vedle sebe dva systémy řízení, a to funkční a procesní, což činí řízení složitějším. Procesní řízení používá obecný proces „Problem Solving Process“, který je součástí best-practice (dobré praxe, tj. nejlepších zkušeností) a je celosvětově široce užíván. Jedná se o obecný proces, který sestává z deseti bodů: identifikace problému; definice problému; analýza současného stavu; hledání příčin; definice cílového stavu; návrh řešení; výběr řešení; validace řešení; realizace; a vyhodnocení.

Procesy pro podporu bezpečnosti jsou v oblasti technické, ekonomické, vzdělávací, lidských zdrojů, komunikace, řízení, administrativy, dokumentace, dozoru, výzkumu atd. Aby bylo dosaženo nejvyšší účinnosti, tak:

- procesy v jednotlivých oblastech musí být koordinované, a proto se v každé oblasti zřizuje proces řízení bezpečnosti, který zajišťuje koordinaci a maximální efektivnost (PSM – process safety management),
- všechny oblasti musí být koordinované, a proto každý subjekt má systém řízení bezpečnosti, který požadavek zajišťuje (SMS – safety management systém).

Procesy řízení bezpečnosti určují způsoby vypořádání rizik ve prospěch chráněných zájmů, tj. určují opatření a činnosti prevence, připravenosti, odezvy, obnovy a způsoby reakce na neočekávané situace. Jelikož nejúčinnější jsou technická opatření v oblasti prevence, je zřejmé, že technické vědy musí připravovat příslušné zázemí. Uvedené tvrzení podporuje požadavek na výběr nejlepších dostupných technik (BAT – best available technology), což znamená, že dané zařízení je projektováno a konstruováno, udržováno, provozováno a rušeno tak, že riziko nebo potenciál způsobit škodu jsou vypořádány ve prospěch chráněných aktiv bez ohledu na náklady s tím spojené.
Pro zajištění druhého požadavku je nutné, aby si inženýři ze všech technických oborů, systémoví inženýři, IT specialisté, ekonomové, personalisté a další specialisté vzájemně rozuměli, protože jen tak mohou zajistit celkový cíl. Uvedený fakt ukazují, že pro řízení bezpečnosti projednávané záležitosti patří do všech základních vědních oborů, tj. sociálních, environmentálních i technických.

6. Kultura bezpečnosti

Z výše uvedených faktů vyplývá, že úroveň bezpečnosti je určená kvalifikovaností lidských opatření a činností a kvalifikovaností jejich implementace do praxe. Kultura bezpečnosti je výrazem sdílení hodnot a opatření systému řízení bezpečnosti a je základním prvkem pro řízení bezpečnosti. Odráží koncepci bezpečnosti a vychází z hodnot, stanovisek a jednání vrcholových řídících pracovníků 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 jsou zapracována do všech činností v území nebo jiné entitě. 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.
V souvislosti s kulturou bezpečnosti se často v současné odborné literatuře spojené s technologiemi používají pojmy prevence ztrát a procesní bezpečnost. Jde o nástroje, které slouží ve spojitostech s technologiemi k ochraně osob i majetku. Prevence ztrát (Loss Prevention) je systematický přístup k prevenci (předcházení) havárií nebo k minimalizaci jejich dopadů. Zahrnuje prostředky pro eliminaci zdrojů rizik nebo omezení pravděpodobnosti jejich realizace a pro zmírnění dopadů spojených s touto realizací (preventivní a následná opatření). Dále zahrnuje identifikaci vhodných kontrolních opatření, identifikaci a aplikaci vhodných nápravných opatření, kterými se zajišťuje bezpečná entita mající příslušnou úroveň bezpečí a udržitelného rozvoje a nepředstavující nepřijatelné nebezpečí pro své okolí.
Procesní bezpečnost nebo lépe bezpečnost procesů, což je v souladu s anglickým pojmem “Process Safety”, je odvětví bezpečnosti zaměřené na bezpečnost v průmyslu, ve kterém je řada výrobních a přídavných procesů, které jsou nutné k vytvoření konečného produktu daného průmyslu. Jde přitom o zabránění vzniku havárií, které mají zvláštní a charakteristické rysy pro daný specifický průmysl. Zabývá se např. prevencí bezprostředních úniků chemických látek nebo energií ve škodlivém množství, a v případě, že se tyto úniky vyskytnou, tak omezením jejich velikosti, dopadů a následků. Nezahrnuje otázky klasické bezpečnosti a ochrany zdraví při práci, tj. zabývá se čistě technickými problémy, čímž se liší od integrální bezpečnosti systému. Fakta opět ukazují, že projednávané záležitosti patří do všech základních vědních oborů, tj. sociálních, environmentálních i technických

7. Závěr

Ze současného poznání a výše uvedených skutečností vyplývá, že bezpečnost a řízení bezpečnosti jsou mnoha oborové a mezioborové disciplíny, jejich záležitosti patří do všech základních vědních oborů, tj. sociálních, environmentálních i technických. Základním důvodem je skutečnost, že pro zajištění bezpečnosti a její kvalifikované řízení je třeba spolupráce inženýrů z technických oborů, systémových inženýrů, IT specialistů, ekonomů, personalistů, úředníků veřejné správy a politiků, protože jen tak lze ve spolupráci s obyvateli ve funkci občanů, zaměstnanců i aktivistů zajistit celkový cíl, které předmětné disciplíny v zájmu lidí sledují.

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

[1] EU: *FOCUS project study – FOCUS website* http://www.focusproject.eu/documents/14976/-5d763378-1198-4dc9-86ff-c46959712 f8a
[2] US: *The National Strategy For The Physical Protection of Critical Infrastructures and Key Assets*. 2003; http://www.whitehouse.gov/pcipb/ physical _strategy.pdf
[3] FEMA: *Promoting Critical Infrastructure Protection by Emergency Managers and First Responders.* Nationwide. 2005. www.usfa.fema.gov
[4] R. Anderson.: *Security Engineering – a Guide to Building Dependable Distributed Systems.* ISBN 978-0-470-068552-6, J. Willey 2008, 1001p.
[5] R.Bris, Soares, C. G., Martorell S. (Eds): *Reliability, risk and safety*: *Theory and Application*. ISBN: 978-0-415-55509-8, 2367p., CD ROM - ISBN: 978-0-203-85975-9, CRC Press / Balkema, Leiden 2009.
[6] Ch. Bérenguer, Grall A., Soares C. G. (Eds): *Advances in Safety, Reliability and Risk Management.* Taylor & Francis Group, London 2011, ISBN 978-0-415-68379-1, 3068p.
[7] EU: *Risk Assessment and Mapping Guidelines for Disaster Management*. Working paper SEC(2010) 1626. Brussels 2010.
[8] OECD: Assessing Societal Risks and Vulnerabilities. *OECD Studies in Risk Management*. Paris 2006, 276p.
[9] H. E. Roland, Moriarity, B.: *System Safety Engineering and Management.* ISBN 0-471-6186-0. J. Willey 1990, 321p.
[10] W. E. Blatz: *Human Security-Some Reflection*. University of Toronto, Toronto, 1966.
[11] W. Stein, B. Hammerli, H. Pohl, R. Posch (eds): *Critical Infrastructure Protection – Status and Perspectives*. Workshop on CIP, Frankfurt am Main, www.informatik2003.de
[12] *Workshop on Critical Infrastructure Protection and Civil Emergency Planning-Dependable Structures, Cybersecurity, Commnon Standard*. Zurich 2005, Centre for International Security Policy, www.eda.admin.ch
[13] C. S. Holling: *Resilience and Stability of Ecosystem.* Annual Review of Ecology and Systematics , 4 (1973) No 1.
[14] L. Gunderson, C. S. Holding: *Panarchy: Understanding Transformation in Human and Natural Systems*. Washington, Island Press 2002.
[15] N. W. Adger: *Social and Ecological Resilience*. Progress in Human Geography 24, (2000) No 3.
[16] F. Langeweg, E. E. Espeleta: *Human Security and Vulnerability in a Scenario Context*. 2001, HDP Update 2.
[17] US NAS: *Framework for Vulnerability Analysis in Sustainability Science.* Proceeding of National Academy of Science, 100 (2010), 14.
[18] K. Dow: *Exploring Differences in Our Commnon Future*. Geoforum 23 (1991) No. 3.
[19] M. Glantz: *Global Warming and Environmental Change*. 1992, Global Environmental Change 2.
[20] J. Smithers, B. Smit: *Human Adaptation to Climatic Variability and Change*. 1997, Global Environmental Change 7 (2).
[21] IAEA: *Safety Guides*. IAEA, Vienna 1954-2010.
[22] OECD: *Guiding Principles on Chemical Accident Prevention, Preparedness and Response.* OECD, Paris 2003, 192p.
[23] 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*. OECD, Paris 2002, 191p.
[24] ISO: Draft International Standard ISO/DIS 31000, *Risk management – Principles and guidelines on implementation*, 2008, 18 p.
[25] EMA: Process of process Safety Management. 2006 www.ema.gov
[26] PetroChem: *Loss Prevention.* PCHE – PetroChemEng, Praha 2004, ISBN 80-02-01574-6, CD ROM
[27] F. P. Lees: *Loss Prevention in the Process Industries*. Butterworths, London 1980.
[28] A. Kossiakoff, W. N. Sweet: *Systems Engineering. Principles and Practices. ISBN 0-471-23443-5.* J.Wiley, New Jersy 2003, 459p.
[29] J. F. Gustin: *Disaster & Recovery Planning: a Guide for Facility Managers*. The FairMont Press, Inc., ISBN 0-88173-323-7 (FP), 0-13-009289-4 (PH). Lilburn 2002, 304p.
[30] WHO/Europe: *REHRA Methodology (Rapid Environment and Health Risk Assessment*. http://www.euro.who.int/watsan/CountryActivities/20030729_11.
[31] Ch. Lucas: *Quantifying Complexity Theory.* 2006, www.calresco.org/lucas/quantity. htm
[32] R. A: Mayers: *Encyclopedia of Complexity and Systems Science*. ISBN 978-0-387-75888-6. Springer, Berlin 2009.

[33] R. Filippini, A. Silva: *A Modelling Language for the Resilience Assessment of Networked Systems of Systems.* In: Advances in Safety, Reliability and Risk Management. CRC Press, Taylor & Francis Group, a Balkema Book, ISBN 978-0-415-68379-1 – Hbk, pp 2443-2450.
[34] G. Ropohl: *Philosophy of socio-technical systems*. In: Society for Philosophy and Technology, 4 (1999), No 3.
[35] J. Moteff, C. Copeland, J. Fischer: *Critical Infrastructures: What makes an Infrastrucuture Critical?* Report for Congress, 2003, CRS Web, Order Code RL31556.
[36] CISP: *Workshop on Critical Infrastructure Protection and Civil Emergency Planning-Dependable Structures, Cybersecurity, Commnon Standard*. Zurich 2005, Centre for International Security Policy, www.eda.admin.ch
[37] S. M. Rinaldi, S.M. (2004): *Modeling and Simulating Critical Infrastructures and Their Interdependencies.* In: Proceedings of the 37th Hawaii International Conference on System Sciences – 2004. Sandia National Laboratories. Sandia. Web: http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1265180
[38] S.M. Rinaldi, J.P. Peerenboom, T. K. Kelly: *Critical Infrastructure Interdependencies. (Identifying, Understanding, and Analyzing).* In: IEEE Control Systems Magazine, Vol. 21, December 2001, pp.12-25. Web: www.ce.cmu.edu/~hsm/im2004/readings/CII-Rinaldi.pdf
[39] A. Kuhlmann: *Does Safety Science Fulfill the Requirements of Modern Technical Systems?* In: Safety of Modern Systems. Congress Documentaion Saarbruecken 2001. Cologne : TŰV- Verlag GmbH, 2001, ISBN 3-8249-0659-7, p. 9-17.
[40] H. J. Pasman, J. K. Vrijling: *Social Risk Assessment of Large Technical Systems*. In Safety of Modern Systems. Congress Documentaion Saarbruecken 2001. Cologne : TŰV- Verlag GmbH, 2001, ISBN 3-8249-0659-7, p. 151-162.
[41] R. R. Fullwood: *Probabilistic Safety Assessment in the Chemical and Nuclear Industries.* Boston : Butterworth Heinemann 2000, p. 514 ISBN 0-7506-7208- 0
[42] OCHA: *OCHA Orientation Handbook on Complex Emergencies*. OCHA, Geneve 2000.
[43] COMAH: *Safety Report Assessment Manual: COMAH*. London : UK- HID CD2 London 2002, 570 p.
[44] ASCE: *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*". ASCE, Washington 2001.
[45] SAIC: *A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection*. National Cooperative Highway Research Program Project 20-07/Task 151B, Science Applications International Corporation–Transportation Policy and Analysis Center, Vienna 2002.
[46] ISM: *International Safety Management (ISM) Code 2002*. IMO, London 2002.
[47] J. Althoff: *Preface. In Safety of Modern Systems*. Congress Documentaion Saarbruecken 2001. Cologne : TŰV-Verlag GmbH, 2001, ISBN 3-8249-0659-7, p. 5-6.
[48] W. Geysen: *The Acceptance of Systemic Thinking in various Fields of Technology and Consequences on Respective Safety Phylosophies*. In Safety of Modern Systems. Congress Documentaion Saarbruecken 2001. Cologne : TŰV-Verlag GmbH, 2001, ISBN 3-8249-0659-7, p. 19-27.
[49] A. R. Hale: *Safety management in Production.* In Safety of Modern Systems. Congress Documentaion Saarbruecken 2001. Cologne : TŰV- Verlag GmbH, 2001, ISBN 3-8249-0659-7, p. 383-392.
[50] E. McGuinwess, I. B. Utne, M. Kelly: *Development of a Safety Management System for Small and Medium Enterprises (SME's).* In: Advances in Safety, Reliability and Risk Management. CRC Press, Taylor & Francis Group, a Balkema Book, ISBN 978-0-415-68379-1 – Hbk, pp 1791-1799.
[51] AS/NZS (2004): *Australia and New Zealand Standard: Risk Management, issued by Standards.* Australia, Guideline 4360. http://www.riskmanagement. com.au/Default.aspx?tabid=148 –116 pp.
[52] US: *Federal Response Plan* 9230.1-PL.
[53] EU. *Green Paper on European Programme for Critical Intrastructure Protection*. Brusel 17.11.2005, COM(2005) 576.
[54] M. Dunn, I. Wiegert: *Critical Information Infrastructure Protection*. International CIIP Handbook. ETH, Zuerich 2004, 405p.
[55] EU: *ESRAB Report: A Report from the European Security Research Advisory Board*. EU, Brussels 2006, 95p.
[56] EU: *ESRIF Final Report.* EU 2009, 319p.
[57] US: *US Critical Infrastructure Conception*. Washington 2001.
[58] EMA: *Critical Infrastructure Emergency Risk Management and Assurance.* Handbook Emergency Management Australia, 2003, www.ema.gov.au
[59] PSEPC: *Assets criteria***.** Public Safety and Emergency Preparedness Canada**,** Ottawa, Canada. 20 January 2004. Web: www.psepc.gc.ca/prg/em/nciap/assets_criteria-en.asp
[60] Bundesministerium des Innern: *Protection of Critical Infrastructures – Baseline Protection Concept.* Recommendation for Companies. Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Zentrum Schutz Kritischer Infrastrukturen, Bonn 2006. www.bmi.bund.de
[61] EEA: *Late lessons from early warnings: the Precautionary Principle 1896-2000.* European Environmental Agency. Environmental issue report No 22, Copenhagen, 2001. http://reports.eea.eu.int/environmental_issue_report_2001_22/en/tab_content_RLR
[62] DoD US: *DoD Security Engineering Facilities Planning Manual*. Department of Defense US. DRAFT UFC 4-020-01, 3 March 2006. http://www.wbdg.org/ndbm /DesignGuid/pdf/FINAL%20DRAFT_UFC_4-020-01.pdf

[63] J. Ludwig Konersmann J., Peinelti R: *Safety Considerations for the Transport and Storage of Dangerous Goods, based on the Example of Pipelines*. Federal Institute for Materials Research and Testing (BAM), Berlin 2002. Publ. NATO-Committee on the Challenges of Modern Society. http://www.pal.metu.edu.tr/projeler/natoccms/CCMS_report_252_Annex.doc
[64] EU (2006). *The Seventh Frame Research Programme 2007-2013*.Brussels.
[65] UN (1994). *Human Development Report*. New York: UN, 1994, www.un.org.
[66] UNEP: *Caring for the Earth. A Strategy for Sustainable Living*. IUCN/UNEP/WWF Gland, Switzerland, 1991, 2006.
[67] D. Procházková: *Strategické řízení bezpečnosti území a organizace*. ISBN: 978-80-01-04844-3. ČVUT, Praha 2011, 483p
[68] Bossel, H. (2004). *Systeme, Dynamik, Simulation – Modellbildung, Analyse und Simulation komplexer Systeme*. Books on Demand, Norderstedt/Germany, ISBN 3-8334-0984-3, www.libri.de.

ADRESA AUTORA:

doc., RNDr. Dana PROCHÁZKOVÁ, PhD., DrSc., České vysoké učení technické v Praze, Fakulta dopravní, Ústav bezpečnostních technologií a inženýrství, Konviktská 20, 110 00 Praha 1, prochazkova@fd.cvut.cz

RECENZIA TEXTOV V ZBORNÍKU
Recenzované dvomi recenzentmi, členmi vedeckej rady konferencie. Za textovú a jazykovú úpravu príspevku zodpovedajú autori.

REVIEW TEXT IN THE CONFERENCE PROCEEDINGS
Contributions published in proceedings were reviewed by two members of scientific committee of the conference. For text editing and linguistic contribution corresponding authors.