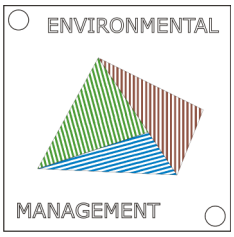
RUSKO, M. – BALOG, K. [Eds.] 2007:
Manažérstvo životného prostredia 2007 ▼▲▼ Management of Environment ´2007
zo VII. konferencie so zahraničnou účasťou konanej 5. - 6. 1. 2007 v Jaslovských Bohuniciach
Proceedings of the International Conference, Jaslovské Bohunice, 5-6 January 2007
Žilina: Strix et VeV. Prvé vydanie. ISBN 978-80-89281-18-3.



NÁSTROJ PRO HODNOCENÍ RIZIKA SYSTÉMU SYSTÉMŮ

DANA PROCHÁZKOVÁ

TOOL FOR RISK ASSESSMENT OF SYSTEMS SYSTEM

ABSTRAKT
Pro řízení věcí veřejných je nutné znát rizika systému systémů, který je souborem vzájemně propojených podsystémů. Důsledkem závislostí jsou spletité řetězce nežádoucích jevů, které vznikají při selhání jednoho či více podsystémů. Pro systém systémů lze poměrně jednoduše stanovit integrované riziko, které však nezohledňuje vzájemnou závislost podsystémů, a proto není příliš vhodné pro řízení. Určení integrálního rizika, které je určeno systémovým přístupem znamená stanovení časově a místně specifického řešení pro systém systémů. Vhodným nástrojem pro jeho určování a pro rozšíření znalostí v příslušné oblasti se jeví zpracování případových studií.
Klíčová slova: *Systém systémů. Vzájemná závislost. Integrované a integrální riziko. Případová studie.*

ABSTRACT
For public affairs governance there are necessary to know the risks of the systems system that is a set of dependable subsystems. The results of dependences there are confused chains of unfavourable phenomena that originated at failure of one or more subsystems. For systems system there is possible relatively simply to determine the integrated risk that does not consider dependability among subsystems, and therefore, it is not too suitable for governance. The determination of integral risk assessed by system approach means an assignment of time and site specific solution for systems system. Suitable tool for its determination and for knowledge enlargement at appurtenant domain there are appeared the case studies processing.
Key words: *Systems system. Dependability. Integrated and Integral Risk. Case Study.*

1. Úvod

Základním cílem řízení věcí veřejných je zajistit v lidském systému přijatelnou úroveň bezpečí, které v sobě inherentně obsahuje dostatečnou úroveň udržitelného rozvoje. Protože nelze zanedbat skutečnost, že lidské zdroje jsou omezené a soubor opatření „bezpečnost“, který zajišťuje bezpečí něco stojí, tak bezpečí odpovídá stavu lidského systému, ve kterém mezní náklady na prevenci se rovnají mezním nákladům na odstranění škod způsobených pohromami (tj. nákladům na odezvu a obnovu). Takto definovaná úroveň bezpečí je ekonomickým optimem pro lidský systém.
Nástroje řízení jsou normativní, ekonomické, etické a institucionální. Opírají se o monitoring, soustavu indikátorů pro posuzování účinnosti aplikovaného souboru opatření a o cíle existujících a ustavených procesů v lidském systému. Správné řízení zajišťuje zvyšování účinnosti souboru opatření

tak, aby docházelo k růstu ekonomického potenciálu a tím i ke zvyšování konkurenceschopnosti institucí i států.
Správné řízení věcí veřejných zaměřené na bezpečí a udržitelný rozvoj je řízení bezpečnosti mající formu procesního a projektového řízení, které je koordinované z úrovně státu [1,2]. Pro potřeby řízení bezpečnosti a rozvoje území se monitorují úroveň bezpečí, pohromy, existující ohrožení, rizika apod. a připravují se podklady pro rozhodování tak, aby se zajistila bezpečná komunita, bezpečné území, bezpečný stát atd. Řízení věcí veřejných se opírá o kvalifikované plánování a zahrnuje v nejobecnějším pojetí vedení, správu, ovládání a úřední projednávání věcí důležitých pro bezpečí a udržitelný rozvoj. 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 celku, tj. státu / území / objektu / organizace apod. [1].
Z hlediska současného poznání řízení věcí veřejných má tři propojené úrovně, a to strategické řízení, řízení procesů a operativní řízení. Zvlášť důležité je řízení procesů, které není rutinní, ale je procesem řešení problémů (Problem Solving Process), které se důsledně opírá o řízení rizik ve prospěch bezpečí a udržitelného rozvoje v dynamicky se měnícím světě. Rizika se vypořádávají ve prospěch bezpečnosti (Risk Governance). To znamená, že při řízení bezpečnosti se používá optimální soubor opatření na vypořádání se s riziky s cílem zajistit bezpečí a udržitelný rozvoj chráněných zájmů s ohledem na dostupné zdroje, síly a prostředky, přičemž respektuje princip předběžné opatrnosti. To znamená, že operativní řízení zaměřené na plnění jednotlivých funkcí je koordinováno v rámci, který je určen cílem stanoveným v procesu, do kterého funkce spadají. Řízení procesů (procesní řízení) je koordinováno v rámci, který je určen cílem stanoveným v projektu, do kterého procesy spadají. Řízení projektů (projektové řízení) je koordinováno v rámci, který je určen cílem stanoveným v programu, do kterého projekty spadají. Programy jsou stanoveny a koordinovány strategickou koncepcí pro rozvoj sledovaných oblastí [1].
Z výše uvedeného vyplývá, že základem procesního, projektového i programového řízení je vypořádání rizik ve prospěch bezpečnosti. Jelikož v praxi nyní často řešíme problémy systému systémů (lidský systém, systém kritická infrastruktura, životní prostředí, lidská společnost, člověk apod.), tak se budeme dále zabývat hodnocením rizik v těchto případech.

2. Charakteristika systému systémů

Problém řízení bezpečnosti lidského systému, systému kritická infrastruktura, životní prostředí, lidská společnost, člověk apod. spočívá v tom, že sledované systémy se skládají ze vzájemně propojených podsystémů. ***Je důležité si uvědomit, že vzájemné propojení znamená závislost.*** Bezpečnost každého systému či podsystému chápaná jako soubor opatření, kterými se zajišťuje bezpečný systém či podsystém, který se může udržitelně rozvíjet, pochopitelně závisí na naturelu systému či podsystému a inherentně v sobě zahrnuje ochranu předmětného systému či podsystému. ***Bezpečnost systému, který je souborem vzájemně závislých podsystémů je předurčená nejen bezpečností jednotlivých podsystémů, ale také charakterem vzájemných propojení.***
Podle práce [3] ***propojitelnost*** znamená závislost *mezi aspoň dvěma podsystémy. Prostřednictvím tohoto spojení stav jednoho podsystému ovlivňuje nebo koreluje se stavem jiného podsystému.* Uvedenou definici lze ještě rozšířit o podmínku vzájemného sdílení některých fyzických prvků nebo procesů, přičemž tyto prvky nebo procesy mohou být situovány v určité územní oblasti. Proto vzájemná závislost v území může být fyzická, kybernetická, logická a územní. Přitom platí:

1. Dílčí podsystémy jsou fyzicky vzájemně závislé, jestliže stav jednoho z nich je závislý na materiálním výstupu podsystému druhého.
2. Kybernetická vzájemná závislost znamená, že stav jednoho podsystému závisí na informacích z jiného podsystému. Kybernetická vzájemná závislost předpokládá existenci informačního podsystému.

3. Podsystémy jsou územně vzájemně závislé, jestliže události v území mohou měnit stavy podsystémů.
4. Logická vzájemná závislost znamená, že stav jednoho podsystému závisí na stavu jiného podsystému, přičemž mechanismus propojení není fyzický, kybernetický nebo územní. Jedná se o závislosti přenášené přes toky, kterými jsou předpisy, finance, legislativa apod., např. se může jednat o finanční trhy.

V důsledku vzájemné závislosti porucha či selhání jednoho podsystému způsobí poruchu či selhání podsystému druhého. Tento fakt přispívá ke kritičnosti systému, který je souborem podsystémů. Proto nestačí zajišťovat podsystémy odděleně, ale je třeba zajišťovat celý soubor podsystémů systémově, což v praxi znamená hledat řešení problému ***BEZPEČNOST SYSTÉMU SYSTÉMŮ*** [4].

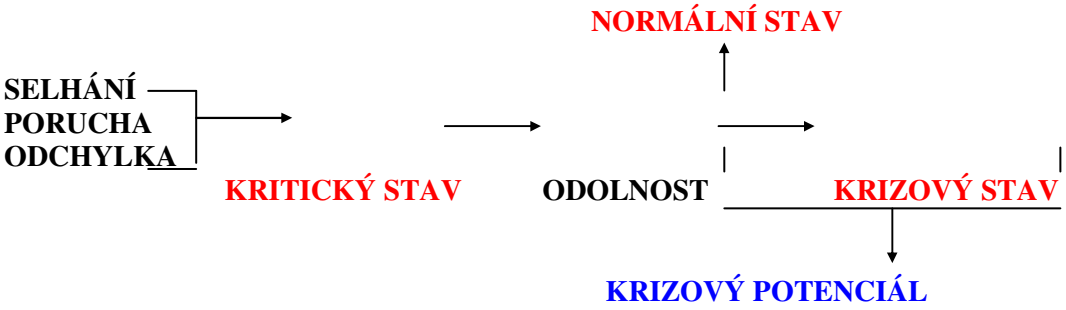
Realitou je, že každý podsystém i celý soubor takovýchto podsystémů je složitý dynamický systém s určitou úrovní přizpůsobivosti. Pro zajištění jeho stability a funkčnosti se musí znát prahová hodnota – kritičnost, která určuje stav, při kterém systém nezajišťuje očekávané funkce v požadovaném čase, místě a v požadované kvalitě. Při aplikaci poznatků z řízení bezpečnosti systému systémů [4] je soubor podsystémů v území kritický, když je pouze schopný zajistit činnosti, při kterých je ještě zajištěno přežití lidí v území. K tomuto účelu je třeba udělat analýzy podsystémů, sledovat vzájemné závislosti mezi podsystémy a řízení bezpečnosti systému systémů zaměřit tak, že respektuje jak podmínky funkčnosti pro jednotlivé podsystémy, tak podmínky nutné pro funkčnost systému, který je souborem podsystémů.

3. Vlastnosti, které ovlivňují chování podsystémů i systému

Z hlediska cílů řízení věcí veřejných nás především zajímá chování subsystémů i systému, který je souborem vzájemně propojených podsystémů. Jde o to, jak je spolehlivá stabilita chování podsystémů i systému, který je souborem vzájemně propojených podsystémů. Spolehlivost (dependability) podsystému i systému, který je souborem podsystémů, ***znamená, že podsystém či systém plní stanovené požadavky po stanovenou dobu při zachování stanovených parametrů podsystému či systému.*** Tato souhrnná vlastnost je pro analytické účely nepraktická, a proto se rozkládá do dvou základních vlastností, kterými jsou zranitelnost a odolnost. K dosažení určité úrovně spolehlivosti podsystémů i systému, který je souborem podsystémů se musí zvážit jednat zranitelnosti od možných pohrom (u systému, který je souborem podsystémů včetně závislostí vyvolaných vzájemným propojením) a jednak schopnosti a možnosti člověka zajistit jistou odolnost.

Odolnost je třeba chápat jako jistou funkční schopnost podsystému či systému, který je souborem podsystémů *plnit úkoly i za abnormálních a kritických podmínek. Pro dosažení tohoto stavu je nutné, aby podsystémy či systém, který je souborem podsystémů měly určitou adaptační kapacitu.*

Spolehlivost je projektovanou vlastností a vztahuje se nejen k normálnímu stavu, ale i ke stavům abnormálním a kritickým, ve kterých prostřednictvím adaptační kapacity subsystémů či systému, který je souborem podsystémů zajišťuje žádoucí reakce i při určitých typech kritických stavů. V antropogenní oblasti jsou obvykle v projektování, výstavbě a provozování zváženy kritické stavy očekávané, tj. předvídatelné, jejichž dopady by byly vysoce nepřijatelné (tj. uplatňuje se princip předběžné opatrnosti). Nicméně mohou nastat kritické stavy, které jsou nepředvídatelné nebo jsou důsledkem závažné chyby obsluhy a ty mohou přejít do nežádoucích / nepřijatelných, tj. i krizových stavů, viz obrázek 1. Krizový potenciál se dá vyjádřit jako současné působení spouštěcího faktoru (spouštěcích faktorů) a nestabilních podmínek prostředí podsystému či systému, který je souborem podsystémů.



Obr. 2. Vztah mezi kritickým a krizovým stavem

Podobně jako u rizika se hodnotí pravděpodobnost jeho výskytu, tak i u krizového potenciálu se hodnotí pravděpodobnost výskytu krizového stavu, a to včetně hodnocení jeho dopadů, které se chápou ve formě závažnosti narušení funkcí částí a procesů subsystému či systému, který je souborem podsystémů.
Ze spolehlivosti vyplývá, že podsystémy či systém, který je souborem podsystémů, jehož podsystémy hrají klíčovou roli ve společnosti, protože ovlivňují rozhodovací cyklus veřejné správy a politickou a sociální soudržnost a napomáhají v odstraňování fyzických a psychických škod, je velmi složitá, a tudíž zranitelná. Proto by se v hodnocení měly vždy charakterizovat a popisovat tři základní vlastnosti podsystémů či systému, který je souborem podsystémů, a to:

- pružná odolnost (resilience),
- zranitelnost,
- schopnost adaptace.

Jelikož každý podsystém či systém, který je souborem podsystémů je složitý socio-technický systém, který obecně má toky hmoty, energie a informací a zpětné vazby včetně recyklů), tak níže uvedené definice na tento přístup reagují:

1. ***Pružná odolnost:***

Pružná odolnost je schopnost podsystému či systému absorbovat a využít odchylky a změny tak, že přetrvá ve své funkčnosti, aniž by došlo ke kvalitativním změnám jeho struktury [5].
Pružná odolnost je mírou takového rozsahu odchylek, které systém může absorbovat před přechodem z jednoho stavu do jiného [6].
Pružná odolnost je mírou rychlosti návratu systému do rovnovážného stavu [6].
Pružná odolnost je rozsah odchylek, které systém může absorbovat, aniž by se změnila jeho stabilita [6].
Pružná odolnost určuje přetrvávání reakcí v systému a je mírou schopnosti systému absorbovat změny stavu [7].
Pružná odolnost je mírou rychlosti zotavení se z odchylek [8].

2. ***Zranitelnost:***

Zranitelnost se vyjadřuje jako vztah mezi expozicí (vystavení) podsystému či systému ohrožení od vnější činnosti a schopností snížit riziko v určitém čase [9].
Zranitelnost je míra zkušeností systému, subsystému nebo prvku se škodami, ke kterým dojde při vystavení škodlivému jevu, který vyvolá stressor (pohroma) nebo odchylka [10].
Zranitelnost vyjadřuje míru mezi vystavením systému či podsystému nenadálým jevům a zátěži, a obtížností, která je spojená s jejich zvládnutím [11].
Zranitelnost vyjadřuje schopnost systému či podsystému reagovat na výskyt škodlivé nežádoucí události [12].
Zranitelnost je výsledkem kombinace vystavení, odolnosti a pružnosti [13].

3. ***Adaptace:***

Adaptace se vztahuje k neplánované reaktivní odezvě systému či subsystému na události nebo podmínky s cílem vyhnout se nepřijatelným dopadům prostřednictvím předjímajících reakcí [14].
Adaptace zahrnuje změny v systému nebo podsystému jako výsledek reakce na projevy vnějších sil nebo odchylek [15].
Při projektování subsystémů jsme zatím z pohledu zajištění bezpečnosti lidského systému řešili problém zajištění funkčnosti jednotlivých subsystémů. Z hlediska současného poznání před námi dnes stojí minimálně dva následující úkoly:

1. Řešit problém funkčnosti souboru vzájemně propojených (tj. závislých) subsystémů (tj. systému systémů) za normálních, abnormálních a kritických podmínek.
2. Vyhledat kritické stavy systému systémů, které jsou nepředvídatelné nebo jsou důsledkem závažné chyby obsluhy a za jistých podmínek mohou přejít do vysoce nežádoucích a vysoce nepřijatelných stavů, tj. do stavů, ve kterých je ohrožena samotná existence lidí a které obvykle označujeme jako krizové.

Proto se dnes u systému systémů posuzuje pružná odolnost (resilience), zranitelnost a schopnost adaptace s tím, že:

- ***pružná odolnost*** systému systémů *je mírou schopnosti* systému systémů *absorbovat změny stavu vyvolané možnou pohromou (včetně interakcí),*
- ***zranitelnost*** systému systémů *je neschopnost* systému systémů *reagovat na výskyt možné pohromy (včetně interakc)í,*
- ***adaptace*** *kritické infrastruktury je schopnost* systému systémů *přizpůsobit strukturu prvků, vazeb a toků systému systémů tak, aby dopady pohromy (včetně interakcí) nebyly pro systém systémů nepřijatelné.*

4. Metodika pro hodnocení rizika systému / podsystému

Riziko vyjadřuje pravděpodobnou velikost nežádoucích / nepřijatelných dopadů (ztrát, škod a újmy) pohromy o velikosti ohrožení na chráněné zájmy systému či podsystému za stanovený časový interval (např. 1 rok) v určitém místě (je vždy místně specifické). Slovo pohroma je používáno v obecném smyslu a zahrnuje všechny jevy, interakce i činnosti, které působí nebo mohou způsobit nežádoucí chování systému či podsystému, jehož důsledkem jsou ztráty, škody, selhání funkčnosti, výpadky činností apod.
Riziko závisí jednak na ohrožení a jednak na zranitelnosti chráněných zájmů v daném místě (tj. na citlivosti každého jednotlivého chráněného zájmu v daném místě vůči fyzikálním projevům pohromy v daném místě). Vyjadřuje možnost toho, co by se mohlo stát, viz údaje shrnuté v pracích [15-17]. Z uvedené skutečnosti vyplývá, že pro každé řízení je důležité znát riziko, a to v pochopitelném vyjádření. V praxi veřejné správy se osvědčilo vyjádření rizika ve formě údaje, že na základě analýzy a hodnocení rizik v území bylo zjištěno, že na specifikovaném úseku:

- je třeba 5 miliónů každý rok na nápravu škod, způsobených existujícím rizikem,
- každých 10 let zemře 10 lidí v důsledku sledované pohromy,
- každých 5 let škody na majetku způsobené pohromou přesáhnou 5 miliard.

Metody pro stanovení velikosti rizik respektují jak podstatu jevů, které jsou jejich zdrojem (tj. charakteristiky a fyzikální podstaty pohrom), tak parametry prostředí, ve kterém se jevy vyskytují. Používají se metody založené na matematické statistice, mlhavých množinách, přístupech operační analýzy apod., které inherentně předpokládají určitý model výskytu jevů, tj. nepřipouštějí, že tyto jevy jsou mimořádné i metody založené na scénářích simulovaných nebo empirických, viz údaje shrnuté v práci [15]. V zásadě lze rozdělit dva základní přístupy, a to:

1. Určení ohrožení od pohromy H a periody návratu τ (v rocích) metodami založenými na teorii velkých čísel, teorii extrémů, teorii mlhavých množin, teorii chaosu, teorii fraktálů apod. Podle místní zranitelnosti chráněných zájmů v definovaném území (např. čtverec 10 x 10 km; kružnice o

poloměru 5 km) stanovit celkovou škodu pro ohrožení H (v penězích) označenou S. Riziko R je pak dané vztahem

$$R = \frac{S}{\tau}. \qquad (1)$$

2. Určení scénáře pohromy o velikosti největší očekávané pohromy (lze podle požadavků normativu použít pravděpodobnou velikost očekávané pohromy nebo hodnotu normativně stanovené pohromy nebo nejméně příznivé pohromy) a dle dat pro dané území určit:
   - podle chráněných zájmů a jejich zranitelnosti vůči dopadům ve scénáři pohromy určit celkovou škodu zasaženého území (v penězích) S,
   - podle odborných údajů z databází nebo expertních odhadů určit četnost výskytu největší očekávané pohromy normovanou na 1 rok f.

   Riziko R je pak dané vztahem

$$R = S * f. \qquad (2)$$

Slabinou při stanovení rizika je skutečnost, že na rozdíl od vyspělých zemích v České republice chybí křivky zranitelnosti chráněných zájmů vůči možným pohromám [16-17], a to znamená, že zranitelnost se musí oceňovat metodou „případ od případu“, která je zdlouhavá a může způsobit neporovnatelnost výsledků.

Pro řízení systému potřebujeme integrální riziko spočtené dle vztahu (1) nebo (2), a to pro všechny možné pohromy, které přispívají k narušení systému systémů. Pro stanovení integrálního rizika systému, které odráží všechny možné pohromy, které přispívají k narušení systému systémů lze použít součet rizik spočtených pro každou pohromu podle vzorce (1) nebo (2) a nebo lze použít indexovou metodu takto:

1. Nechť i=1,2,…, n je počet chráněných zájmů sledovaného systému. Za předpokladu, že každý chráněný zájem obsahuje s_i elementů, které ho tvoří, platí, že:

   $s_{i,j}$ je j-tý element i-tého chráněného zájmu, tj. j = 1, 2, …, s_i.

2. Nechť $h_{i,j}$ – množství pohrom, které ohrožují element $s_{i,j}$, pak platí, že:

   $h_{i,j,k}$ je k-tá pohroma v i-tém chráněném zájmu pro j-tý element, tj. lze položit k´=1,2,… $h_{i,j}$.

Na základě odhadu míru zranitelnosti konkrétních elementů chráněných zájmů při jednotlivých pohromách určíme riziko vztahem:

$$R_{i,j,k} = P_{i,j,k} \cdot D_{i,j,k}, \qquad (3)$$

ve kterém $P_{i,j,k}$ je pravděpodobnost výskytu a $D_{i,j,k}$ je dopad. Zvolíme-li stupnici rizika následujícím způsobem:

0 – riziko bezvýznamné, zanedbatelné,
1 – riziko malé, okrajové,
2 – přijatelné riziko pod hranicí platných standardů,
3 – podmíněně přijatelné, tj. tolerovatelné riziko, které je redukovatelné běžným systémem odezvy,

4 – významné riziko, tj. riziko nad hranicí standardů, které je redukovatelné připraveností a speciálním systémem odezvy,
5 – nepřijatelné riziko

lze index rizika $I_{i,j}$ pro i-tý chráněný zájem a j-tý element lze stanovit jako vážený průměr individuálních indexů pro jednotlivé pohromy

$$I_{i,j} = \sum_{k=1}^{h_{i,j}} w_{i,j,k} \,.\, I_{i,j,k} \text{ s tím, že } \sum_{k=1}^{h_{i,j}} w_{i,j,k} = 1, \text{ přičemž}$$

$w_{i,j,k}$ je váha indexu rizika k-té pohromy pro j-tý element i-tého chráněného zájmu.
Když index rizika i-tého chráněného zájmu je I_i, tak

$$I_i = \sum_{j=1}^{s_i} w_{i,j} \,.\, I_{i,j} \text{ s tím, že } \sum_{j=1}^{s_i} w_{i,j} = 1$$

Pro celý systém je index rizika všech chráněných zájmů od pohrom roven

$$I = \sum_{i=1}^{n} w_i \,.\, I_i \text{ s tím, že } \sum_{i=1}^{n} w_{i,} = 1, \text{ přičemž}$$

hodnoty vah, které značí významnost odpovídajících indexů lze stanovit analytickým nebo expertním způsobem.
Integrální riziko systému, které vyjadřuje pravděpodobnou velikost nepřijatelných dopadů (ztrát, škod a újmy) všech možných pohrom, které přispívají k narušení systému systémů dostaneme pomocí vztahu (3). Zase je třeba připomenout, že pro snadné pochopení je dobré vyjádřit velikost dopadů v peněžních jednotkách.

4. Návrh postupu pro hodnocení rizika systému systémů

Na základě vzorců (1) nebo (2) lze zjistit jak rizika jednotlivých podsystémů, tak riziko celého systému. Integrované riziko R_{IN} je potom dáno vztahem

$$\mathbf{R_{IN} = \sum_{i=1}^{l} R_i} \,, \qquad (4)$$

ve kterém R_i pro i=1,2,...,l jsou rizika dílčích podsystémů. Při zvážení n možných pohrom, které přispívají k narušení systému systémů je potom celkové integrované riziko R_{CIN} od pohrom určeno vztahem

$$\mathbf{R_{CIN} = \sum_{r=1}^{n} R_{INr}} \,, \qquad (5)$$

Integrované riziko stanovené dle vztahů (4) a (5) je však v důsledku propojitelnosti podsystémů nevhodné pro řízení, protože nedává odhad o skutečném stavu věcí, tj. neodráží vliv propojitelnosti

podsystémů, které působí, že u každého chráněného zájmu jsou dopady přímé i dopady způsobené propojitelnosti podsystémů.
Vzhledem k tomu, že příklady z praxe ukazují, že vlastnosti podsystémů (odolnost, zranitelnost a schopnost adaptace) ve sledovaných systémech jsou místně a časově specifické [5-13,18], je třeba hledat časově a místně specifické řešení. Takováto řešení lze získat např. aplikaci metodiky na stanovení případových studií [19].

5. Závěr

Realitou je, že každý systém i celý soubor systémů (systém systémů) je složitý dynamický systém s určitou úrovní přizpůsobivosti. Pro zajištění jeho existence, funkčnosti i bezpečnosti je třeba znát jeho rizika. Riziko systému systémů je časově a místně specifické. Proto je obtížné najít obecné řešení. Na základě analýzy možných nástrojů pro podporu rozhodování a řízení navrhujeme pro stanovená území zpracovat komplexní případové studie a pomocí jejich výsledků prověřit např. možné časově a místně specifické relace mezi vztahy (3) a (5) a shromáždit údaje o časových a místních variacích v odolnosti, zranitelnosti a ve schopnosti adaptace podsystémů i celého systému.
Ke zvýšení bezpečnosti systému systémů přispívá také rychlá a účinná odezva na selhání systému systémů a také rychlá a účinná obnova funkčnosti podsystémů, což znamená, že nestačí znát rizika, ale je třeba vědět jak s nimi vyjednávat ve prospěch bezpečnosti.

ZOZNAM BIBLIOGRAFICKÝCH ODKAZOV

[1] D. Procházková: *Principy správného řízení věcí veřejných s ohledem na bezpečí.* Sborník „Integrovaná bezpečnost 2007“, MTF STU, Trnava 2008, v tisku.
[2] K. Lacina: *Regionální rozvoj a veřejná správa*. ISBN 978-80-86754-74-1, VŠFS, Praha 2007, 70p.
[3] W. Stein, B. Hammerli, H. Pohl, R. Posch (eds): *Critical Infrastructure Protection – Status and Perspectives*. Workshop on CIP, Frankfurt am Main, www.informatik2003.de
[4] D. Procházková, K. Balog: *Bezpečnost systému systémů*. In: Environmentálne aspekty požiarov a havárií. ISBN 978-80-8096-052-0, EAN 9788080960520. STU – Mtf, Trnava 2008, 11p.
[5] C. S. Holling: Resilience and Stability of Ecosystem. Annual Review of Ecology and Systematics , 4 (1973) No 1.
[6] L. Gunderson, C. S. Holding: *Panarchy: Understanding Transformation in Human and Natural Systems*. Washington, Island Press 2002.
[7] S. Franklin, T. Downing: *Resilience and Vulnerability*. GECAFS Project, Stockholm Environment Institute 2004.
[8] N. W. Adger: *Social and Ecological Resilience.* Progress in Human Geography 24, (2000) No 3.
[9] F. Langeweg, E. E. Espeleta: *Human Security and Vulnerability in a Scenario Context.* 2001, HDP Update 2.
[10] *Framework for Vulnerability Analysis in Sustainability Science*. Proceeding of National Academy of Science 100 (14).
[11] R. Chambers: *Vulnerability, Coping and Policy*. IDS Bulletin. 20 (1990) No. 2.
[12] J. M. Watts, G. H. Bohle: *The Space of Vulnerability*. Progress in Human Geography 17 (1993) No. 1.
[13] K. Dow: *Exploring Differences in Our Commnon Future.* Geoforum 23 (1991) No. 3.
[14] M. Glantz: *Global Warming and Environmental Change*. 1992,Global Environmental Change 2.
[15] D. Procházková: *Integrální, integrovaná a dílčí bezpečnost.* ISBN 80-7312-054-2, MV ČR THEMIS, Praha 2008, 60p.

[16] D. Procházková, J. Říha: *Krizové řízení*. MV-GŘ HZS ČR, ISBN 80-86640-30-2, Praha 2004, 225p.
[17] D. Procházková: *Bezpečnost a krizové řízení*. ISBN 80-86477-35-5. POLICE HISTORY, Praha 2006, 255p.
[18] J. Smithers, B. Smit: *Human Adaptation to Climatic Variability and Change*. 1997, Global Environmental Change 7 (2).
[19] D. Procházková: *Případová studie a metodika pro její sestavení*. Sborník „Integrovaná bezpečnost 2007“, MTF STU, Trnava 2008, v tisku.

ADRESA AUTORA

doc. RNDr. Dana Procházková, DrSc., Policejní akademie ČR v Praze, Praha, Česká republika

RECENZENT

prof. Ing. Karol Balog, PhD., Slovenská technická univerzita v Bratislave, Materiálovotechnologická fakulta Trnava, Ústav bezpečnostného a environmentálneho inžinierstva, Botanická 49, 917 01 Trnava, Slovenská republika, e-mail: >karol.balog@stuba.sk<