KRITICKÁ INFRASTRUKTURA A VEŘEJNÁ SPRÁVA

CRITICAL INFRASTRUCTURE AND PUBLIC ADMINISTRATION

Jaroslav MOZGA
jaroslav.mozga@ioolb.izscr.cz

Abstract

Current society is in such a degree dependent on infrastructure functions that it is inevitable to analyze the role of public administration in protection of critical infrastructure. It proves, at the same time, that it is necessary to take a think about the definitions of critical infrastructure, as they are too static and consider carefully if the concept of critical social functions is not more suitable. The article briefly describes the risk management and protection of critical infrastructure with the emphasis that it is desirable to devote the attention to the concept of resilient society. Public administration should, in connection with protection, seriously deal with the organizational development and processes of control of changes which would lead to the implementation of strategic and integrated risk management. No less important task of pubic administration is to renew its credit to the public.

Key words
Risk management, critical infrastructure, integrated risk management.

Požadavek správného fungování infrastruktury společnosti není ničím novým, jak se lze dozvědět z historie. Římské impérium nebo středověké čínské císařství jsou příklady společností, jež znaly důležitost společenské infrastruktury, a proto ji ochraňovaly vojenskou silou nebo náboženstvím. A pakliže společenská infrastruktura přestala plnit své funkce, došlo ke kolapsu. Příkladem budiž kolaps římského impéria, které se rozpadlo především z vnitřních příčin (nefunkční infrastruktura státu) a nájezdy barbarů rozpad jen dovršily.

Moderní společnost závisí na dobře fungující infrastruktuře, zejména technologické (dodávky vody a potravin, dodávky elektřiny a tepla, dodávky pohonných hmot, komunikace, mobilita apod.)**,** a jejíž nefunkčnost by měla neblahé dopady na naplnění **základních lidských potřeb** (zdraví, bezpečí) a **kvalitu lidského života** (majetek a prosperita, spotřeba energií a potravin, ochrana krajiny, majetku a prostředí). Technologická infrastruktura a infrastruktura řízení státu tak tvoří **infrastrukturu společnosti**, kterou lze charakterizovat následovně:

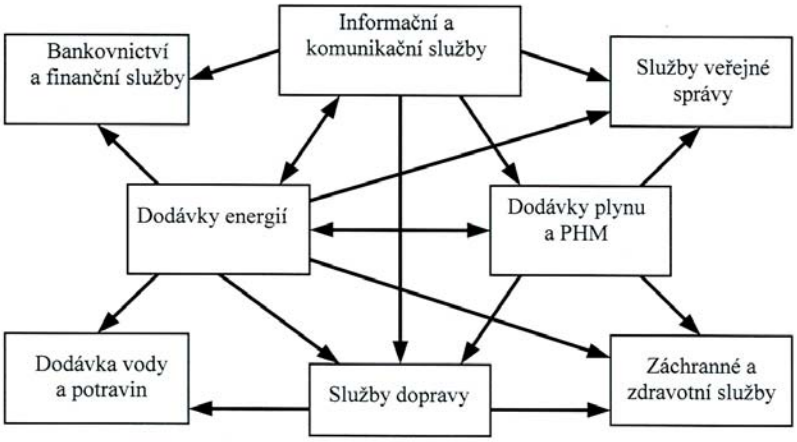
- Současná společnost je **zcela závislá na normálním průběhu operací** technologické infrastruktury (produkty a služby) a infrastruktury řízení státu (veřejné služby) a tato závislost znamená **sníženou odolnost** vůči nepříznivým jevům.
- Jednotlivé infrastruktury současné společnosti jsou **vzájemně provázané**, čímž se zvyšuje jejich složitost a vnímavost vůči poruchám.
- Snížení zranitelnosti složitých systémů vyžaduje značné finanční prostředky, jichž je samozřejmě nedostatek.

- Deregulace rozdělila infrastruktury mezi různé vlastníky.
- Civilizované prostředí, jako forma technologické infrastruktury, se snaží přebírat některé funkce za přírodu, a proto se musíme stále více a více chránit proti vlivům prostředí, v němž žijeme.
- Každá infrastruktura poskytující produkty nebo služby využívá **prostředky informačních technologií**, což vede k centralizaci řízení z důvodů automatizované kontroly a supervize, přičemž klesá odolnost digitálních systémů vůči poruchám.

Ze společenského hlediska se kritickou infrastrukturou rozumí vzájemně propojené sítě či systémy obsahující identifikovatelná odvětví a instituce (včetně lidí a postupů) poskytující spolehlivý tok produktů a služeb podstatných pro obranu a ekonomickou bezpečnost, která se chápe jako schopnost státu konkurovat na globálních trzích, zatímco se udržují na přijatelné úrovni reálné příjmy obyvatel a fungování veřejné správy na všech úrovních společnosti. K ekonomické bezpečnosti se připojuje i bezpečnost fyzická týkající se ochrany fyzických aktiv před škodami v důsledku působení fyzických sil a bezpečnost kybernetická zabývající se především ochranou před poruchami nebo neautorizovanými přístupy do počítačových sítí.

V souvislostí s kritickou infrastrukturou již nejde jen o výjimečné situace ohrožení životů a státu, nýbrž jde také o zachování běžného provozu společnosti, a proto se musí hledat stav, při němž infrastruktura neposkytuje služby v požadovaném čase a v požadované kvalitě.

V definici kritické infrastruktury se odrážejí zkušeností a zvyklostí států: *záplavy (Holandsko), problém národní obrany (Francie, Švédsko, Nový Zéland), problém hi-tech kriminality (Itálie - legislativa, poštovní a komunikační technologie), problém ohrožení rozvoje informační společnosti (Finsko), problém ohrožení podnikatelských aktivit (Švýcarsko, Anglie), problém boje proti terorismu (Nový Zéland, USA).*



Obr. 1
Obecné schéma kritické infrastruktury

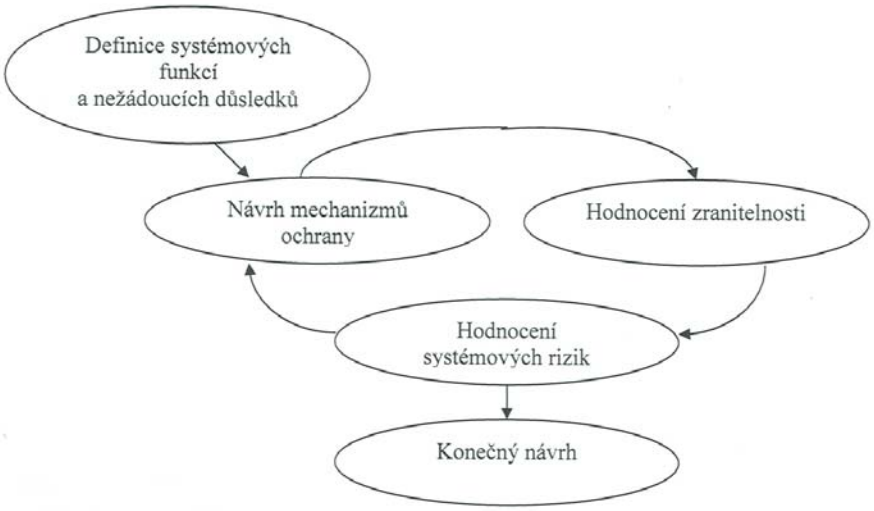
Někdy se místo pojmu kritická infrastruktura používá pojem „život podporující sítě“ (lifeline support network). Tento pojem propaguje zejména Austrálie a Nový Zéland, naopak Finsko používá pojem „vitální funkce“ a ve Švédsku se vžil pojem „kritické společenské funkce“ (critical societal functions), což jsou takové funkce ve společnosti, že jejich přerušení nebo porucha může vést ke stavu nouze ve společnosti. Kritické společenské funkce závisí na situaci a proto není možné vytvořit v předstihu jejich univerzální seznam. Švédský přístup se dá nazvat jako přístup orientovaný na důsledky (criticality of consequences).

Poznámka. Ke kritičnosti lze přistupovat z hlediska teleologického a systémového:

- *Z **teleologického hlediska** plyne, že kritičnost je důsledkem role a funkcí infrastruktury ve společnosti. Tento koncept umožňuje pracovat s nesíťovými a netechnickými objekty a procesy.*
- *Infrastruktura je ze **systémového hlediska** kritická v důsledku svého postavení v systému nebo vazby na jiné infrastruktury.*

Řízení rizik kritické infrastruktury [4]

Proces řízení rizik je v literatuře dostatečně popsán, nicméně řízení rizik kritické infrastruktury vyžaduje systémový přístup, protože se předpokládá, že funkcionalita celku se vztahuje k subsystémům a prvkům – činnost každého prvku závisí na tom, do jaké míry „vyhovuje“ celku, a účinnost celku je podmíněna fungováním jednotlivých prvků.



Obr. 2
Kroky v řízení rizik kritické infrastruktury

Se zřetelem na organizaci a řízení musí proces řízení rizik infrastruktury splňovat tyto vlastnosti: ***schopnost predikce problémů*** (identifikace), ***schopnost predikce dopadů*** (analýza), ***schopnost plánovat, schopnost realizovat akce*** (monitorování a snížení rizik)**.**

Úlohou řízení rizik je zabránit výskytu nebo odstranit příčiny a zmírnit důsledky nežádoucích jevů působících na systém daného typu. V odlišném postavení je **správa rizik** (risk governance), odkazující se na vyšší úrovně řízení. Základní rozdíl mezi řízením a správou rizik spočívá v počtu aktivních účastníků zahrnutých do identifikace, návrhu a realizace opatření vůči riziku, a s jistou nadsázkou se dá říci, že správa rizik je „syntézou" řízení rizik jednotlivých aktivních účastníků. Postup správy rizik je podobný postupu řešení problému v manažerské praxí a sestává z těchto částí:

1. **Formulace problému**
   Každý aktér má různý pohled na daný problém, a je tudíž žádoucí, aby se ke každému zúčastněnému přistupovalo otevřeným a rovnocenným způsobem.
2. **Preference řešení**
   Každý zúčastněný podle svého hodnotového systému a své definice problému hodnotí možná řešení a zkoumá jeho parametry jako jsou *náklady, vedlejší účinky, účinnost a účelnost.*
3. **Rozhodování**
   Řeší se rozdílnosti a konflikty s cílem najít konzistentní a přijatelné řešení. Kromě toho se definuje odpovědnost za řešení včetně práv a povinností všech zúčastněných.
   V rámci rozhodování se zjišťují *možné alternativy* pro řízení rizik (technické, organizační, legislativní apod.), které se *kriteriálně hodnotí* a uspořádané varianty se *hodnotově konsolidují* před konečným rozhodnutím.
4. **Dohoda nebo kompromis**
5. **Realizace politiky veřejné správy a její sledování**

Ochrana kritické infrastruktury [4]

Ochrana kritické infrastruktury svádí dohromady značný počet existujících strategií, plánů a procedur zabývajících se prevencí, připravenosti a odezvou a obnovou. Nejedná se o novou disciplínu, jedná se spíše o koordinaci existujících disciplín jako jsou *krizové řízení, plánování kontinuity podnikání, řízení bezpečnosti, řízení rizik, strategie udržitelného rozvoje, ochrana obyvatelstva* (civilní ochrana, civilní obrana) apod.

Ochrana kritické infrastruktury vyžaduje aktivní účast vlastníků a operátorů, regulátora, profesních asociací a institucí ochrany obyvatel. Pro tuto spolupráci by měly platit tyto zásady:

1. Ochrana kritické infrastruktury by se měla soustředit na minimalizaci zdravotních a bezpečnostních rizik pro veřejnost a měla by napomoci kontinuitě podnikání a kontinuitě služeb veřejné správy.
2. Měly by se využívat vhodné postupy a techniky řízení rizik pro určení úrovně **bezpečné ochrany** (ochranné bezpečnosti) a pro nastavení priorit alokace zdrojů.

Obr. 3
Veřejná služba a kritická infrastruktura

3. Kritická společenská funkce je vhodným východiskem pro strukturování ochrany do tří vrstev:
   - **vrstva fyzická**
   (systém řízení bezpečnosti vlastníka/operátora)
   - **vrstva provozní**
   (*organizační kultura*)
   - **vrstva strategická**

   ŘÍZENÍ UTILITY

   (*veřejná správa se zabývá dopady na obyvatele – social impact assessment, vlastník analyzuje možnosti plánování životního cyklu aktiv utility)*
   Utilita je prvkem kritické infrastruktury poskytujícím veřejné služby a podléhající regulačním opatřením veřejné správy. Z ekonomického hlediska se jedná o přirozené monopoly.

Obr. 4
Vztah utility a obyvatelstva

Koncept ochrany je svým způsobem dehumanizující, poněvadž se primárně zaměřuje na provozní spolehlivost technických systémů a inženýrskou resilienci (resilience se obecně chápe jako **pružná odolnost**), která se vztahuje k rychlosti obnovy a týká se stability systému. Koncept vitálních funkcí (Finsko), kritických společenských funkcí (Švédsko) a sítě život podporujících funkcí (Nový Zéland) však upozornil na nezbytnost analyzovat nejen technický systém, ale i systém sociální a ekonomický, které jsou cílem ochrany.

Nicméně až hurikán Katrina přinesl posun v myšlení – mělo by se přejít od **ochrany** kritické infrastruktury k **resilientní komunitě**. V současnosti je koncept resilience komunity výrazem reálné připravenosti komunity a její schopnosti nejen účinně a účelně reagovat na pohromu, nýbrž také se z důsledků pohromy zotavit. Důvod tohoto posunu je zjevný – život komunity je úzce spjat s ekonomickým blahobytem a bezpečným prostředím.

Krizová připravenost [4]

„Připravenost je velké bohatství a štěstí“ říká buddhistické učení. Tato filozofická metafora však musí být nějak operacionalizována, aby připravenost se stala skutkem. Cílem připravenosti je vždy snížení účinků nežádoucích dopadů a urychlená obnova (zotavení). Avšak není připravenost jako připravenost, což lingvisticky přesně ukazuje angličtina:

- **Připravenost** (preparedness) znamená vycvičenost v procedurách a systémových postupech a vybavení odpovídajícími přístroji.
- **Připravenost** (readiness) souvisí s prací (profesní pozice) a vyjadřuje vysokou motivaci, pochopení poslání a porozumění rizikům.

Z výše uvedených přístupů lze usuzovat, že **krizová připravenost** neznamená **jen vědět co dělat a jak dělat** v krizové situaci, ale znamená také **motivaci, odbornou úroveň a profesní a profesionální odpovědnost.**

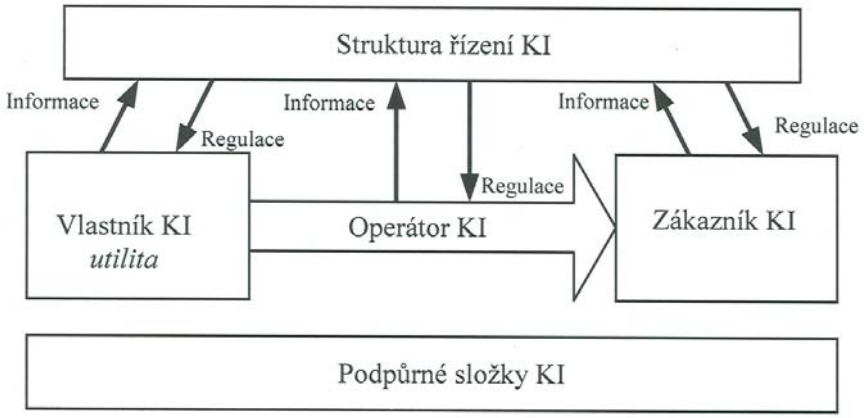
Krizová připravenost kritické infrastruktury se netýká jen vlastníků (operátorů) utilit kritické infrastruktury, ale týká se také veřejné správy a institucí ochrany obyvatelstva a svým způsobem se také dotýká obyvatelstva. Krizová situace kritické infrastruktury se chápe jako **situace, v níž bezprostředně nějaká změna, která je vážnou hrozbou sociálnímu systému, a vyžaduje kritická rozhodnutí za časového tlaku a nejistých okolností**.

Krizové situace může vyvolat vlastník, politické rozhodnutí, neschopnost veřejné správy apod. Proto je důležité při analýze připravenosti analyzovat technické, ekonomické, lidské, organizační a sociální faktory, jež mohou zapříčinit krizovou situaci. Analýza vlivu lidských faktorů odráží limity lidské racionality (způsoby uvažování) a předpojatost vůči informacím, které jsou v rozporu s jinými informacemi nebo vlastními přesvědčením, nepochopení povahy krizové situace, problémy rozhodování za stresu apod. Jako příklad uvádíme klasifikaci krizových situací pro vlastníka utility kritické infrastruktury:

Faktory	*Vnitřní krizové situace*	*Vnější krizové situace*
Technické/ekonomické	Havárie zařízení Narušení informační a komunikační technologie (ICT)	Živelní pohromy Destrukce životního prostředí
	Defektní informace	Selhání veřejné správy
Lidské/organizační/sociální	Sabotáž insiderů Nepřizpůsobivost vůči změnám prostředí	Sabotáž z vnějšku (outsideři) Terorismus

Krizová připravenost není vyplňováním tabulek v dikci právních vyhlášek, krizová připravenost je procesem, jenž se skládá z *monitorování trendů vnějšího prostředí* (informační management), *plánování s využitím scénářů, stanovení rizik, včasného varování a z účinného rozhodovacího procesu* (návrh organizace rozhodování na základě rozhodovací analýzy).

Role veřejné správy a ochrana kritické infrastruktury



Obr. 5
Vztahy v kritické infrastruktuře

Veřejná správa je v nelehké situaci neboť musí rozhodovat o ochranných opatřeních ve složitém prostředí (vztah rizika a bezpečí) na složitých systémech a složitých situacích:

Charakteristiky jednoduché situace	*Charakteristiky složité situace*
Situace je jasně ohraničená a lze ji zkoumat izolovaně	Situace je ohraničena nejasně a neurčitě
Obsahuje soubor entit/událostí	Obsahuje soubor entit/událostí, které se nemohou rozumně zkoumat izolovaně nebo se týká skupin a institucí s nejasnými rolemi a záměry
Informační potřeby jsou známy	Informační potřeby se musí definovat
Problémy v situaci jsou buď známé nebo je možné je popsat	Problémy jsou buď „záludné“ (wicked) anebo jsou vnořené
Kauzální vztahy jsou poměrně stabilní	Kauzální vztahy se mohou měnit dynamicky nebo strukturálně a obtížně se zjišťují
Změny jsou kvantifikovatelné a dají se deterministicky predikovat	

Situace jsou složité, protože současná infrastruktura je složitější (vzájemné závislosti, vlivy ICT vyžadující centralizaci) a společnost je méně odolná vůči poruchám – chod společnosti zcela závisí na normálním provozu infrastruktur jak lze doložit na těchto příkladech: *třicetišesti hodinový výpadek (2001) švýcarské mobilní sítě v důsledku aktualizace centralizovaného softwaru, čtyřhodinový výpadek (2005) curyšské tramvajové dopravy v důsledku aktualizace centrálního softwaru, tříhodinový výpadek švýcarské železnice (2005) v důsledku nesprávného softwarového hodnocení situace.*

Nepružná organizační struktura, styl řízení a rozhodování, nedostatečná odpovědnost (právní, politická a odborná) a nedostatek vhodných nástrojů se rovným dílem podepisují na chybách rozhodování veřejné správy, jež jsou výsledkem

- **Odloučení od reality** (realita je nepohodlně plna složitých situací)
  Popírání vzájemných závislostí
  Ignorování projevů nebezpečí
  Nedostatečné znalosti a schopnosti – byrokratická kultura bezpečnosti
- **Regulační smyčky systémů se neberou na vědomí**
- **Krize legality** (kvalita zákonů) a z toho vyplývající **rezignace na odpovědnost** (zákon slouží jako krytí)
- **Nedostatky v plánování a strategii**
  Preferuje se reaktivní plánování (interoperabilita) před proaktivním plánováním (simultánní analýza vzájemných závislostí, zranitelnosti, nebezpečí a zdrojů)

Organizace a instituce hrají klíčovou roli ve společnosti. Mají odpovědnost za provozování, udržování a řízení infrastruktury poskytující statky a služby pro obyvatele. Schopnost organizace účelně a účinně reagovat na nežádoucí události závisí na její struktuře, systému řízení a kvalitě řídících pracovníků. Ukazuje se, že u klíčových organizací a institucí je zcela zásadní **schopnost pokračovat v plnění svých funkcí i v případě neočekávaných událostí**.

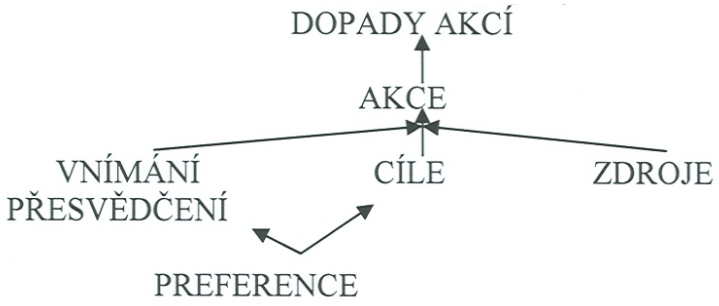
V obecné rovině je resilience výrazem schopnosti rychlé obnovy a zotavení z důsledků pohromy a skládá se ze **zranitelnosti** (snadnost s jakou se systém dostává

do nového stavu) a **adaptivní kapacity** (míra schopnosti zvládat změnu). V případě resilience [3] organizace se k adaptivní kapacitě přidává povědomí o situaci a řízení klíčových zranitelností:

- **Povědomí o situaci** je výrazem vnímání a porozumění organizace svému okolí (schopnost rozpoznat a identifikovat nouzové a krizové situace, porozumění spouštěcím faktorům/prekurzorům, pochopení vztahu zdrojů a obnovy).
  Povědomí o situaci se skládá z vytváření povědomí o resilienci (scénáře důsledků) a výběru kritických organizačních prvků z hlediska vnější a vnitřní perspektivy.
- **Řízení klíčových zranitelností** se zabývá těmi aspekty organizace, provozu a řízení, jež mají potenciál působit negativně v krizové nebo nouzové situaci (jedná se nejen o hmotná aktiva, ale také o aktiva nehmotná – komunikační struktura, vztahy apod.).
  Řízení klíčových zranitelnosti staví na výběru kritických organizačních prvků – identifikuji se hlavní a kritické funkce a požadavky na kontinuitu, hodnotí se zranitelnosti, vnímavost a priorizují se klíčové zranitelnosti.

Kvalita politického rozhodování a rozhodování veřejné správy je výrazem úrovně individuálních a institucionálních schopností. Instituce zabývající se ochranou obyvatel a kritické infrastruktury by měly být schopny **jednat** (rozhodování na základě znalostí – jak systémy různého typu pracují, jaké jsou důsledky), **mít výsledky** (řešení problémů – výsledek je zlepšení stavu), a **být přizpůsobivé** (řízení změn – pochopit význam změn).

Hermans [2] ukazuje na důležitost **analýzy aktivních účastníků** (actors analysis) v řízení infrastruktury a analýzy **sítě zájmových skupin** (policy network) nastavující podmínky pro jednotlivé aktivní účastníky. Síť zájmových skupin se skládá z ***jednotlivých aktivních účastníků*** (jedinec, skupina, organizace), kteří ***mají schopnost rozhodovat a jednat koordinovaným způsobem na základě vzájemných vztahů*** (vztahy hierarchické, konzultativní apod.) a ***pravidel*** (pravidlo je sociálně konstruovaný argument vztahující se k obecným znalostem aktivních účastníků) ovlivňujících chování aktivních účastníků při dosahování výsledků). Samotný aktivní účastník se schematicky popisuje následovně:



Obr. 6
Popis účastníka [2]

Systém řízení veřejné správy a kritická infrastruktura

Veřejná správa je hierarchicky organizovaná a na rozdíl od podnikových struktur se nemění tak často, přestože by se měla organizačně rozvíjet prostřednictvím procesu řízení změn. Německá společnost organizačního vývoje (German Society of Organizational Development) charakterizuje organizační rozvoj jako:

> *Proces změn organizace a lidí, jenž je založen na učení se ze zkušeností. Cílem rozvoje je současné zlepšení produktivity a účinnosti organizace a humanizace pracovního a okolního prostředí. (GOE 1980).*

Organizační rozvoj veřejné správy z hlediska ochrany (obyvatel, prostředí a kritické infrastruktury) by se měl zabývat strategickým a integrovaným řízením rizik:

1. **Strategické řízení rizik**

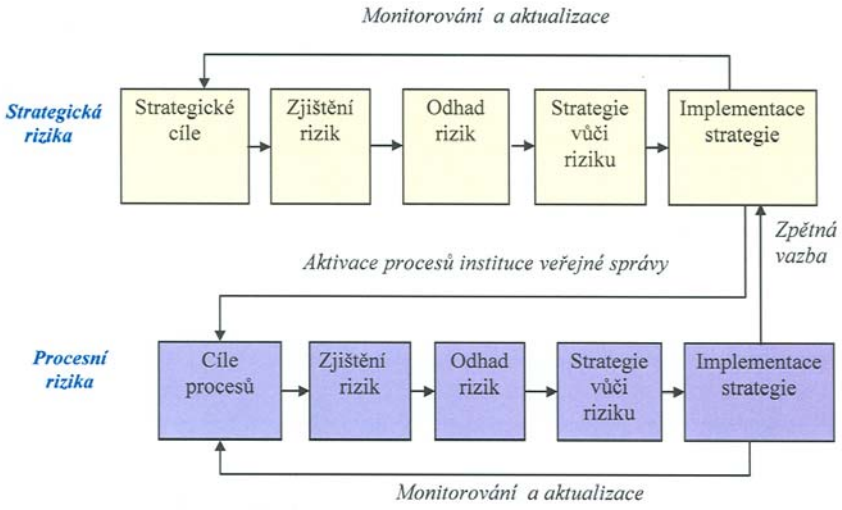
Strategické řízení zdůrazňuje potřebu organizačního přizpůsobování stavu prostředí a přináší do řízení ochrany kritické infrastruktury tyto přínosy [1]:

Přínos	*Popis*
Profesionalita a odbornost	
„Dopředné“, proaktivní myšlení“	Zaměření na budoucnost Strategické plánování Dlouhodobá perspektiva „Skenování“ prostředí
Vytváření kapacit	Kapacity se vytvářejí procesem učení a adaptace Řízení změn Podpora systémového myšlení a schopnosti volit mezi alternativami
Identifikace záměrů a úspěšnosti	Rovnováha mezi centralizaci plánu a decentralizovanou realizací
Zodpovědnost a vyšší podpora veřejnosti	Používá se technika řízení „důsledky-interakce“ a analýza zpětných vazeb

Veřejná správa rozhoduje o ochraně obyvatel, jejíž součástí je bezpečnost/bezpečí jako veřejná služba a toto rozhodování je normativní (regulace, strategie a cíle ochrany) a je politicky formulováno a ovlivňováno, zejména se to týká přijatelnosti rizika. Veřejná správa, ač rozhoduje o tzv. vnějších rizicích, měla by je analyzovat nejen z hlediska společenských dopadů, nýbrž také z hlediska dopadů na systém řízení veřejné správy. Může se totiž stát, že rozhodování může dopady vnější rizikové události jen zhoršit.

Kroky v postupu v řízení rizik veřejné správy se nijak neliší od běžného postupu řízení s tím rozdílem, že se musí věnovat značná pozornost formulaci kontextu a orientaci na strategická a procesní rizika:

- **Strategický kontext** (vztahy mezi institucí veřejné správy a prostředím), Posuzuje se schopnost dosažení strategických cílů v oblasti ochrany a bezpečnosti, mobility a stavu prostředí (zdravotní a environmentální rizika)
- **Organizační kontext** (schopnost instituce řešit problémy),
- **Kontext řízení rizik** (prahová úroveň rizika, maximální úroveň dopadů, priority rozhodování).



Obr. 7
Procesy řízení rizik ve veřejné správě

2. Integrované řízení rizik

Moderní stát hraje roli, která se dá popsat v termínech řízení rizik, protože přerozděluje určité typy rizik prostřednictvím systému blahobytu a zdravotní péče. Rostoucí debaty o riziku na úrovni vládních institucí a veřejné správy je možné vysvětlit jako důsledek uvědomění rizik, kvůli nimž může selhat poskytování veřejných služeb. Nadto veřejnost se může domnívat, že veřejná správa je zdrojem rizik ve špatně zvládaných krizových a nouzových situacích.

Je tedy oprávněné hovořit o „veřejném riziku“, které lze charakterizovat jako výraz procesů, jež jsou důsledkem prosazování partikulárních zájmů pod pláštíkem veřejného zájmu. Rizika vstupují do veřejné oblasti, naplňují-li některý z těchto atributů:

- *Jde o externality, které nemohou řešit tržní mechanizmy.*
- *V souvislosti s individuálními právy jsou občanům vnucovány škodlivé účinky.*
- *Je ohrožena značná část veřejnosti.*
- *Politické rozhodnutí vyvolá rizikovou událost.*
- *Nežádoucí události jsou rozloženy tak, že se nebere ohled na politickou spravedlivost.*

Regulace rizik jako nová politika vůči nejistotě, by měla předpokládat, že selhání, poruchy a havárie jsou ve složitém prostředí možné, dokonce za spoluúčasti expertních omylů a nedopatření. Politika nejistoty proto musí:

- Vzít explicitně na vědomí, že instituce veřejné správy obvykle „vybírají“ rizika jako směsici socio-ekonomických důvodů, aniž by však rizikům porozuměly. Všechny krizové situace veřejné správy se nestanou náhle, nýbrž mají své počátky v selhání řízení rizik veřejnou správou v dlouhodobém horizontu.

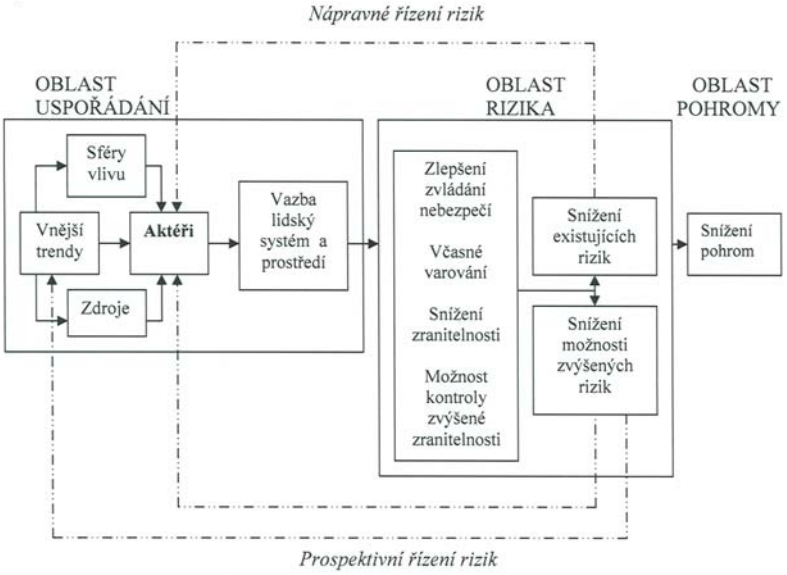
- Vytvořit legitimitu možného selhání a nemělo by se hledat zklidnění obav veřejnosti pomocí rétoriky, že všechna rizika jsou ovladatelná.
- Zajistit nutné institucionální podmínky tak, aby se zvýšila důvěra v rozhodování veřejné správy a důvěra v úsudky neprodejných expertů.

Instituce zabývající se řízením rizik (rizik týkajících se občanů), většinou zcela opomíjejí skutečnost, že jejich **rozhodování je zdrojem rizik**, takže veřejnost má malou důvěru ve stanovení rizik veřejnou správou, protože se neví *jaké faktory ovlivňují rozhodování o rizicích na jednotlivé organizační úrovni institucí, jak se v rozhodování projevují znalosti, přesvědčení, úmysly rozhodovatelů a normativní tlaky.*

Na překonání nedůvěry se využívá koncept integrovaného řízení rizik, což je přístup zahrnující riziko do všech rozhodovacích procesů instituce a na všech úrovních řízení. Cílem integrovaného řízení rizik je

- **zlepšení výsledků rozhodování**,
- **posílení odpovědnosti a zodpovědnosti vůči veřejnosti - řízení rizik je veřejnou službou (statkem)**.
  Riziko je pro občana negativní externalitou- podnikatelské subjekty včetně veřejné správy se často nezabývají dopady určitých činností a jevů na občany.

Příkladem integrovaného řízení rizik je **GIRO rámec (G**estión **I**ntegral de **R**iesg**O),** analyzující vliv **aktérů** (skupiny, instituce), jež rozhodujícím způsobem ovlivňují vazby lidského systému a prostředí. GIRO rámec také upozorňuje na nutnost zvyšovat povědomí o rizicích u rozhodovatelů ve veřejné správy a podílet se na dosažení politické shody o opatřeních.



Obr. 8
Schéma GIRO rámce

Literatura

[1] CHOI, O.S. *Emergency management implications from a strategic management perspective.* Journal of Homeland Ssecurity and Emergency, 5(1), 2008.

[2] HERMANS, M.L. *Actor analysis for water resources management.* Eburg Publishers, Delft, 2005, ISBN 90-5972-091-1.

[3] MOZGA, J., VÍTEK, M. *Riziko, zranitelnost, bezpečí.* Studijní texty k systémové ekologii, Gaudeamus, Hradec Králové, 2008.

[4] MOZGA, J., VÍTEK, M., KOVÁŘÍK, F. *Kritická infrastruktura společnosti.* Gaudeamus, Hradec Králové, v tisku.