ŽILINSKÁ UNIVERZITA V ŽILINE
FAKULTA BEZPEČNOSTNÉHO INŽINIERSTVA
KRÍZOVÝ MANAŽMENT - 2/2017
ISSN:1336 - 0019
str. 70-77

OCHRANA KRITICKÉ INFRASTRUKTURY – PŘÍPADOVÁ STUDIE

CRITICAL INFRASTRUCTURE PROTECTION – CASE STUDY

Petra SKALICKÁ[1]

ABSTRACT:

This article summarizes one of the outputs of the author's research activities, which focuses on the critical infrastructure protection and the possibilities of its development. A presented case study outlines the current state and circumstances (context) of critical infrastructure protection in the Czech Republic in the conditions of a particular subject of critical infrastructure from the public sector and at the same time proposes possible procedures and measures of a systemic approach to develop critical infrastructure protection.

KEYWORDS: *Critical Infrastructure Protection, case study, systems approach, crisis management.*

ÚVOD

Kritická infrastruktura (dále též „*KI*“) má v rámci bezpečnostní politiky státu zásadní význam. Každý její prvek může ohrozit bezpečnost, ekonomické zájmy či samotný chod státu a zasáhnout do každodenního života společnosti. I přes skutečnost, že zranitelnost kritické infrastruktury se zvyšuje optikou vzrůstající proměnlivosti bezpečnostních hrozeb a jejich různorodosti, není ze strany České republiky a jejich gesčních orgánů věnována této oblasti náležitá pozornost. Konkrétně pak odvětví Veřejná správa a organizační složky státu nesilového zaměření, resp. jejich systém řízení bezpečnosti odráží nedostatečný zájem na zajištění ochrany kritické infrastruktury. Tuto situaci ilustruje průzkum autorky článku, která se zaměřila na zajišťování ochrany KI v praxi konkrétního subjektu KI z veřejného sektoru a realizovatelnost systémových opatření a postupů, které navrhla jako možné a vhodné pro zvýšení úrovně zabezpečení, v jeho specifických podmínkách.

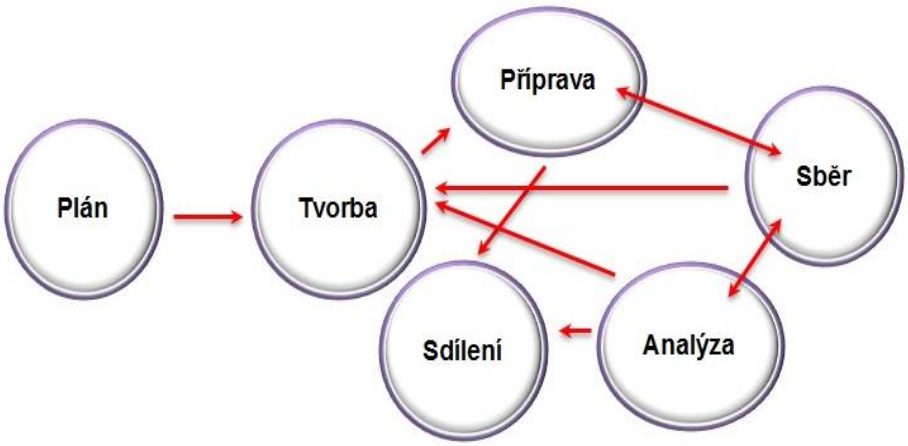
Praktické aspekty ochrany prvku KI jsou podány formou **případové studie**. Důvodem pro výběr této kvalitativní metody je možnost přímého zapojení, načerpání bezprostředních zkušeností a vlastní přínos k rozvoji ochrany KI. Autorce článku byla tato metoda umožněna díky jejímu zaměstnání u tohoto subjektu, a to na pozici styčného bezpečnostního zaměstnance subjektu KI. V rámci případové studie byly využity kombinace různých technik sběru informací, jako například analýza dokumentů (vnitřní předpisy, bezpečnostní dokumentace, výstupy vlastní činnosti – stanoviska, zápisy z jednání apod.), participativní pozorování a nestrukturované rozhovory. Cílem bylo nalezení skutečně realizovatelného řešení a získání zpětné vazby okolí při zavádění opatření. Vedlejším efektem pak osvěta, propagace moderních postupů řízení ve veřejné správě a zlepšení komunikace se všemi zainteresovanými.

1. POPIS VÝZKUMNÉHO ŠETŘENÍ

Výzkumným vzorkem byla **jediná jednotka (objekt)**, a to subjekt KI veřejného sektoru z odvětví Veřejná správa (dále jen „*subjekt průzkumu*“). Tato jednotka byla zvolena jako typický případ (představitel standardu), nikoliv kritický (extrémní či deviantní). Výběr byl účelový, záměrný, neboť se jednalo o zaměstnavatele autorky článku a na počátku výzkumu zde byl předpoklad možnosti dlouhodobého detailního pozorování, který se potvrdil. Studie je výstupem více jak dvouleté činnosti, při níž bylo možno sledovat a přímo participovat na rozvoji ochrany KI ve specifických podmínkách a prostředí. Chyby, ze kterých se učil subjekt průzkumu, jsou inspirativní, stejně tak jako dosažené úspěchy.
Technikou sběru dat tedy byla případová studie [1, 2, 5, 6, 8], ilustrujícího charakteru

[1] Petra Skalická, PhDr., Fakulta bezpečnostního managementu Policejní akademie České republiky v Praze, Lhotecká 559/7, P. O. Box 54, 143 01 Praha 4, Česká republika, e-mail: skalickapetra@post.cz.

(popisná) s potenciálem výzkumného charakteru, kdy by bylo možné formulovat další otázky či hypotézy pro následný například kvantitativní výzkum u širšího vzorku, jak je rozvedeno i v diskusi. Tato metoda se vyznačuje vysokou spolehlivostí, ovšem nízkou reprezentativností výstupů. Ta však byla vyvážena jejich hodnotou výstupů – cennými zkušenostmi při zavádění nových postupů v reálných podmínkách a prostředí, možností pozorovat reakce okolí, změny firemní kultury a přístup k bezpečnosti.



Obrázek 1 **Proces případové studie** [8]

Případová studie probíhala od září 2014 do konce roku 2016, kdy byl prováděn samotný průzkum při pracovní činnosti spočívající v implementaci možných postupů ochrany KI, prosazování změny řízení bezpečnosti, především systémového přístupu. Data a výstupy byly zaznamenávány průběžně formou terénních poznámek.

Doprovodnými technikami výzkumu byly

- *analýza dokumentů*: studium vnitřních předpisů, provozní dokumentace (plány, projekty, směrnice) na ústřední úrovni i územních pracovištích a také případných vlastních výstupů (stanoviska, zápisy z jednání apod.);
- *participativní pozorování*: v rámci vlastní pracovní činnosti autorky (bezprostřední kontakt) byly sledovány reakce okolí na zavedení změny, zaznamenávány bariéry při jejich prosazování, limity legislativní, organizační, finanční, zdrojové, personální apod., úskalí či přínosy vnitřní i vnější spolupráce;
- *nestrukturované, neformální rozhovory*: zejména s bývalými zaměstnanci za účelem pochopení historického kontextu, dále se zaměstnanci zainteresovaných útvarů za účelem pochopení aktuálního kontextu a prostředí a analýzy rizik a také komunikace navenek s gestorem, vnějšími bezpečnostními orgány, odborníky apod.

Předmětem studie je **srovnání stavu před a po realizaci** konkrétních systémových postupů a opatření ochrany KI osvědčených v zahraniční i nejlepší praxí. Výstupem jsou konkrétní realizované kroky, konkrétní posuny subjektu ve snaze zlepšit výkon ochrany KI a tím i úroveň bezpečnosti.

2. POPIS SUBJEKTU PRŮZKUMU

Subjekt průzkumu je státní organizace zřízená vlastním zákonem. Kromě toho, že je organizační složkou státu, je i samostatnou účetní jednotkou, naopak není z povahy vykonávané činnosti správním úřadem, a to ani ústředním správním úřadem, tedy v terminologii krizového zákona [9] nejde o orgán krizového řízení. Svou činnost vykonává subjekt průzkumu také prostřednictvím územních pracovišť, kterých je celkem osm (hlavní město Praha a územní obvody krajských soudů).

Subjekt průzkumu byl určen **prvkem KI** na základě usnesení vlády č. 934 ze dne 14. prosince 2011 [7], a to v souladu s nařízením vlády č. 432/2010 Sb. v odvětví IX. Veřejná správa.

Ode dne určení prvkem KI začala běžet roční lhůta pro zpracování plánu krizové připravenosti (dále jen „*plán KP*“) a měla být realizována opatření k ochraně KI, včetně

plnění zákonných povinností. Kompetentním útvarem v oblasti bezpečnosti, krizového řízení a tedy i v otázkách ochrany KI je samostatné bezpečnostní oddělení tohoto subjektu. Z hlediska organizační struktury je toto oddělení v přímé působnosti generálního ředitele. Vedoucí tohoto oddělení je zároveň bezpečnostním ředitelem v souladu se zákonem č. 412/2005 Sb. [10].

3. HODNOCENÍ STAVU PŘED REALIZACÍ SYSTÉMOVÝCH OPATŘENÍ

Z dostupných interních dokumentů lze hodnotit stav ochrany KI před červencem 2014 jako nedostatečný a neefektivní, což bylo také vyhodnoceno vnitřní metodickou dohlídkou prováděnou nadřízeným ministerstvem, tj. dozorujícím orgánem krizového řízení.

Nedostatky bylo možné spatřovat zejména v následujících klíčových oblastech činnosti:

- *organizace krizového managementu* – nepřehledná organizační struktura krizového řízení, kdy existovala bezpečnostní rada a krizový štáb v téměř totožném složení. Povinnosti těchto orgánů byly nejasně stanoveny. Dle dohledatelných údajů se konalo pouze jedno zasedání bezpečnostní rady. Na úrovni územních pracovišť existovala struktura tzv. prvků krizového řízení ve složení dvou až čtyř referentů (řadových zaměstnanců). Generální ředitel a ředitelé územních pracovišť nebyli nijak do ochrany KI zapojeni. Činnost členů prvku krizového řízení reálně spočívala pouze v občasné aktualizaci kontaktů.
- *plán krizové připravenosti* – bezpečnostní dokumentace byla v rozporu s nařízením vlády č. 462/2000 Sb. [4], její struktura nebyla odpovídající. Věcně obsahovala četné chyby, nadbytečná vágní ustanovení, neaktuální informace. Plán KP byl zdlouhavý, zřídka používaný (pouze pro aktualizaci kontaktů) a nezohledňoval zásadní hrozby a rizika subjektu. Koncept ochrany KI formulovaný v tomto dokumentu byl projevem zásadního nepochopení dané problematiky v podmínkách subjektu. Datum schválení dokumentu neodpovídal roční zákonné lhůtě pro zpracování tohoto dokumentu. Na úrovni územních pracovišť měly být zpracovávány vlastní plány KP, některé však byly rozpracované či zcela chyběly. Zpracované plány pak vykazovaly taktéž rozpor se strukturou danou právními předpisy či obsahovaly zpravidla pouze přehled složení a kontakty na členy prvku krizového řízení.
- *nedostatečná úprava problematiky ve vnitřních předpisech* – problematika ochrany KI či obecně krizového řízení byla upravena pouze ve vnitřním předpisu ke zřízení krizového štábu (příkaz), ke zřízení bezpečnostní rady (rozhodnutí generálního ředitele) a závazném dokumentu Bezpečnostní politika. Tato úprava však spolu ne zcela souvisela, byla nepříliš přehledná, některé její části byly ve vzájemné kolizi. Vnitřní předpisy neobsahovaly úpravu práv a povinností zaměstnanců a vedoucích zaměstnanců, systém krizového řízení či ochrany KI v podmínkách subjektu.
- *kvalifikace odpovědných pracovníků* – za oblast krizového řízení byli odpovědní zaměstnanci bez odpovídajícího vzdělání či odborné způsobilosti v oblasti krizového řízení či bezpečnosti.
- *nízké povědomí zaměstnanců* – v důsledku (nejen) nedostatečné úpravy vnitřních předpisů v oblasti ochrany KI nebylo příliš vysoké povědomí zaměstnanců o dané problematice, ani o základech sebeochrany v krizových situacích (zveřejněna nebyla ani rizika či krizové situace s možnými dopady na subjekt). Dokonce většina členů krizového štábu, bezpečnostní rady či prvků krizového řízení nevěděla o svém členství či povinnostech z tohoto členství vyplývajících.
- *absence spolupráce uvnitř i vně* – vazby z ústředí subjektu na územní pracoviště téměř nebyly funkční. Nepravidelně probíhala kontrolní činnost. Komunikace a spolupráce s gesčním ministerstvem taktéž nebyla četná. Vázla spolupráce s bezpečnostními či výkonnými složkami integrovaného záchranného systému.
- *bezpečnost jako externí služba* – bezpečnostní dokumentace, vnitřní předpisy, případná stanoviska v oblasti bezpečnosti a do jisté míry i další činnost v oblasti bezpečnosti (nejen ochrany KI) byla poptávána a dodávána formou externích (dodavatelských) služeb. Je diskutabilní, zda výše vynaložených finančních prostředků na tyto služby odpovídala kvalitě výstupů. Z pohledu stavu ochrany KI však tento přístup lze hodnotit jako ne zcela vhodný.
- *přehlížení významu ochrany KI, resp. bezpečnosti* – v návaznosti na nízké povědomí o ochraně KI a nedostatečnou informovanost zaměstnanců a především vedení byla problematika bezpečnosti

považována spíše za nedůležitou z hlediska činnosti subjektu a její řešení odsouváno za priority každodenní agendy.

Výše uvedené lze shrnout jako **nepříliš vhodný a dostatečný přístup** k ochraně KI, kterému odpovídal také stav před červencem 2014. **Příčin** je možné nalézt několik: nejednotný výklad zákona, nedostatečná spolupráce uvnitř a vně subjektu, externí služby, nedostatečně kvalifikovaní zaměstnanci, nezájem vedení o danou problematiku, nedostatečná kontrola či absence metodického vedení a spolupráce ze strany orgánu krizového řízení a další. Je třeba poznamenat, že subjekt průzkumu nebyl nucen ve své historii řešit dlouhodobý výpadek či zásadní narušení své funkce, jakožto prvku KI. Povodně v roce 2013 způsobily jisté komplikace, které však byly v krátkém čase vyřešeny. Reálně tedy nebylo možné ověřit nastavený a výše popsaný systém ochrany KI v praxi, tj. při vzniku krizové situace. Neproběhlo ani žádné interní cvičení či cvičení rezortu gesčního ministerstva, kterého by se subjekt účastnil. Školení v oblasti krizového řízení pořádaná gesčním ministerstvem probíhala nepravidelně. Jiná školení zaměstnanci subjektu ani jeho vedení neabsolvovali.

4. PRŮBĚH REALIZACE SYSTÉMOVÝCH OPATŘENÍ K OCHRANĚ KI

Počínaje červencem 2014 došlo v oblasti řízení bezpečnosti subjektu průzkumu k významným změnám. **Personální změny** na pozici vedoucího bezpečnostního oddělení a výměna zaměstnanců na referentských pozicích tohoto oddělení za kvalifikované odborníky předznamenaly zcela nové pojetí agendy bezpečnosti.

Zásadním krokem bylo též **vypovězení dodavatelských smluv** s externími společnostmi poskytujícími služby v oblasti bezpečnosti (poradenská činnost, tvorba plánovací dokumentace, školení apod.). Rok 2015 byl klíčovým pro **tvorbu nového konceptu krizového řízení i řízení bezpečnosti**. Zásluhou kvalifikovaných zaměstnanců bylo možné veškerou činnost zvládnout vlastními silami, aniž by byla jakákoliv služba zajišťována dodavatelsky.

Základem pro zefektivnění ochrany KI bylo **přijetí systémového přístupu**. Nový koncept je založen na srozumitelné strategii zakotvené ve vnitřních předpisech, kompletní přestavbě organizace krizového managementu a zevrubné aktualizaci (přepracování) plánovací dokumentace. V lednu 2015 byl přijat **nový vnitřní předpis** upravující komplexně a přehledně krizové řízení zahrnující ochranu KI.

Vnitřní předpis stanoví základní principy krizového řízení za účelem zajištění přiměřené úrovně bezpečnosti, ochrany života a zdraví zaměstnanců, majetku, ochrany KI a životního prostředí a zajištění kontinuity základních kritických činností a funkcí subjektu včetně jeho ekonomické, personální a materiální stability, dále též práva a povinnosti zaměstnanců, včetně vedoucích zaměstnanců, odpovědnost generálního ředitele a ředitelů územních pracovišť za zajištění připravenosti subjektu, resp. územního pracoviště na krizové situace a mimořádné události, které mohou způsobit narušení či selhání KI, tj. zasáhnout do klíčových činností (funkce). Stanoví též novou organizační strukturu krizového řízení a vazby a vztahy v rámci i vně subjektu v dané oblasti. Zabývá se i krizovým plánováním na ústřední a územní úrovni.

Organizace krizového managementu byla nastavena způsobem, který kopíruje organizační strukturu subjektu. Analogicky k ministerstvům a ústředním státním úřadům byly zřízeny pouze krizové štáby, nikoliv bezpečnostní rady, přičemž krizové štáby plní jak funkci preventivní (poradní orgán při přípravě na krizové situace), tak také reaktivní (pracovní orgán při řešení krizových situací). Krizový štáb subjektu projednává klíčové bezpečnostní dokumenty a navrhuje opatření pro předcházení či řešení krizových situací, která poté předkládá ke schválení generálnímu řediteli. Krizový štáb územního pracoviště je poradním a pracovním orgánem ředitele příslušného územního pracoviště. Tomuto principu je též přizpůsobeno složení krizových štábů, kdy předsedou je vždy nejbližší vedoucí zaměstnanec zastupující ředitele územního pracoviště, resp. na ústřední úrovni náměstek, který je odpovědný generálnímu řediteli.

Tajemníkem je na ústřední úrovni bezpečnostní ředitel a na územní úrovni referent krizového řízení (přímý podřízený ředitele územního pracoviště). Členy krizových štábů jsou vždy vrcholní vedoucí zaměstnanci, kteří předkládají na zasedání krizového štábů požadavky za své útvary. Krizový štáb subjektu je složen ze stálých členů, které zasedají vždy, a dalších členů (rozšířené složení), kteří se připojují v případě operativního svolání krizového štábu, tj. při plnění reaktivní funkce (řešení krizové situace).

Výkonným pracovištěm a sekretariátem krizových štábů jsou **pracoviště krizového řízení**, složené na ústřední úrovni z pracovníků bezpečnostního oddělení, na územní úrovni pak z referenta krizového řízení, a referenta pro bezpečnost a ochranu zdraví při práci a požární ochranu. Vedoucím pracoviště je tajemník krizového štábu, čímž jsou zajištěny úzké operativní vazby na krizový štáb. Pracoviště krizového řízení svou činnost může vykonávat v nepřetržitém provozu. Má srovnatelné postavení jako stálá pracovní skupina orgánu krizového řízení orgánů krizového řízení na lokální úrovni, což se projevuje též při hrozbě vzniku (schylování se) či vzniku krizové situace, kdy se pracoviště stává součásti krizového štábu na příslušné úrovni řízení při jeho zasedání svolaném za účelem řešení takové krizové situace.

Klíčovým nástrojem krizového řízení se stal **plán KP**. I přesto, že určeným prvkem KI je pouze budova v Praze, byla do plánovací činnosti v souladu s ustanovením § 29b odst. 3 krizového zákona[2] zapojena též územní pracoviště, která zpracovávají vlastní dílčí plány KP, jež jsou součástí Plánu KP. Východiskem pro tvorbu plánů byly jak relevantní právní předpisy (zejména nařízení vlády č. 462/2000 Sb.), tak nezávazné normy (Metodika Ministerstva vnitra, Generálního ředitelství Hasičského záchranného sboru ČR ke zpracování plánů krizové připravenosti) [3]. Využito bylo podkladů získaných od gesčního ministerstva, hasičského záchranného sboru, krajských úřadů a dalších, se kterými byli zpracovatelé v přímém kontaktu. Proběhlo několik **školení zaměstnanců** za účelem vysvětlení nového konceptu, pojetí plánovací činnosti a posílení komunikace a vzájemné spolupráce.

Plán KP je v souladu se zákonnými požadavky strukturován do tří částí (základní, operativní a pomocné). Jeho součástí je též statut a jednací řád krizového štábu. Přílohou jsou dále plány spojení, analýza ohrožení a vyhodnocení rizik a též operativní karty, tj. typové postupy a opatření při řešení krizové situace.

Analýza ohrožení byla provedena nejen na základě podkladů od Hasičského záchranného sboru, ale též na základě **vlastní analýzy rizik**, kdy byla identifikována, analyzována a vyhodnocena relevantní rizika krizových situací i některých mimořádných událostí. Ta rizika, která se po provedení hodnocení jejich závažnosti vyznačovala nejvyššími hodnotami (zásadní či nepřijatelné dopady na činnost subjektu), byla předmětem operativního plánování činností pro případ řešení takových situací.

Součástí každého plánu jsou proto **karty s typovými postupy** a návrhy reaktivních opatření. Plány jsou koncipovány tak, aby byly „živou“ dokumentací, praktickou a srozumitelnou pomůckou pro řešení situací umožňující zastupitelnost v případě absence odpovědného pracovníka. Příslušní zaměstnanci je sami zpracovávají, rozumí jim, vědí, kam se podívat v případě hrozby vzniku či vzniku krizové situace. Jsou tak funkčním, věcným, přehledným vodítkem, jehož smyslem je pomoci, nikoliv znásobit stres a generovat zmatečné postupy.

Do konce roku 2015 proběhlo ustavující zasedání krizových štábů, na kterých byly plány schváleny. Následně byla zpracována i další dokumentace, zejména povodňové plány.

Rok 2016 **ověřil systém krizového řízení**, resp. ochrany KI v praxi, kdy byly na úrovni ústředí řešeny z hlediska zajištění klíčových činností subjektu zásadní mimořádné události. Opakovaně zasedal krizový štáb, který se osvědčil jako operativní nástroj vedení subjektu pro řešení mimořádných událostí. Čtvrtletně probíhaly porady s odpovědnými pracovníky z územních pracovišť, kteří se aktivně podíleli na **implementaci nového systému ochrany KI do praxe**. I přes personální změny ve vedení bezpečnostního oddělení je krizové řízení jednou z priorit, a to i z pohledu vedení subjektu.

V roce 2016 byl také sjednocen **systém řízení rizik**. Na něj v roce 2017 naváže nový **systém řízení kontinuity** [11], jehož zatím značnou překážkou je liniové (funkční), tj. nikoliv procesní řízení. Systém ochrany KI se tak neustále vyvíjí a postupnými kroky směřuje k vyšší a udržitelné míře bezpečnosti.

5. HODNOCENÍ ÚSPĚŠNOSTI ZAVEDENÍ SYSTÉMOVÉ OCHRANY KI

Změny realizované v případě subjektu průzkumu v oblasti bezpečnosti, konkrétně ochrany KI, byly ambiciózní, svým způsobem

[2] Ustanovení § 29b odst. 3 krizového zákona: „*Jestliže je prvek kritické infrastruktury členěn do více samostatných celků, může být pro každý takový celek, je-li to účelné, zpracován dílčí plán krizové připravenosti subjektu kritické infrastruktury, který je součástí plánu krizové připravenosti subjektu kritické infrastruktury.*“

i rizikové v případě, že by se nepovedlo některé realizovat, a zároveň i revoluční, neboť cílem bylo vybudovat zcela nový koncept ochrany KI zajišťující funkčnost a schopný řešit krizové situace. Tento cíl byl splněn, jak prokázal rok 2016. Celkové hodnocení však není možné objektivně podat s jednoročním odstupem. Stručný přehled provedených opatření oproti původnímu stavu sleduje tabulka 1.

Tabuľka 1 **Přehled provedených opatření**

PŮVODNÍ STAV (2014)		REALIZOVANÁ OPATŘENÍ
Nepřehledná organizace krizového managementu, nejasné definování povinností a odpovědností	**Systémový přístup/nový koncept krizového řízení (ochrany KI)**	Kompletní přestavba organizace krizového managementu, přesně vymezená práva a povinnosti odpovědných zaměstnanců (vč. členů krizového štábu), zapojení vedení
Neaktuální, chybný, rozporuplný plán krizové připravenosti, nesoulad s právními předpisy, zřídka využívaný		Přepracování plánu krizové připravenosti dle zákonné struktury, víceúrovňové pojetí, zapojení územních pracovišť, důsledná analýza rizik, typové postupy a karty krizových opatření
Nedostatečná úprava ochrany KI ve vnitřních předpisech		Nová strategie, nové vnitřní předpisy, statut a jednací řád krizového štábu
Neodborná kvalifikace odpovědných pracovníků		Personální změny, pravidelná školení, časté porady, cvičení, prvotní seznamování a průběžné informování členů krizového štábu
Nízké povědomí zaměstnanců		Vstupní a průběžné školení zaměstnanců, osvěta
Absence vnitřní i vnější spolupráce		Nastavení komunikačních vazeb a úzké spolupráce vnitřní i vnější
Dodavatelské zajištění ochrany KI		Vypovězení dodavatelských smluv, provádění ochrany KI výlučně vlastními odbornými zaměstnanci
Přehlížení významu ochrany KI (nejen) ze strany vedení		Zapojení vedení, osvěta, prohloubení komunikačních vazeb a vnitřní spolupráce

Reálné a úspěšné výsledky jsou však patrné, **systém je dosud funkční, neustále se vyvíjí a pracuje sám na sobě**. Proces jeho osvědčení v praxi je svou povahou dlouhodobý a je **založen na několika pilířích**:

- *vzájemná spolupráce uvnitř i vně subjektu* (udržování a posilování nejen vnitřní spolupráce, tj. vazeb s územními pracovišti, resp. jednotlivými útvary, ale též vnější – s gesčním ministerstvem, se subjekty KI v rámci jeho rezortu a z jiných odvětví, se zástupci hasičského záchranného sboru a jinými);
- *průběžné (systémové) vzdělávání a podpora připravenosti* (plánovány jsou průběžné semináře pro členy krizových štábů a zaměstnance přímo zapojené do činností krizového řízení, připravují se též společná cvičení, subjekt usiluje o zapojení do cvičení pořádaných státními či lokálními orgány krizového řízení, samozřejmostí jsou čtvrtletní porady);
- *průběžná kontrolní činnost a monitoring* (plánována je kontrolní činnost na územních pracovištích, zpětná vazba je poskytována též při zasedáních krizových štábů, při poradách, konzultacích, metodické činnosti vůči územním pracovištím, průběžně je aktualizována plánovací dokumentace; vnitřní metodická dohlídka ze strany gesčního ministerstva v říjnu 2015 proběhla s konstatováním bezchybného stavu dokumentace i chodu krizového řízení);
- *zvyšování povědomí zaměstnanců* (na intranetu je vytvořen informační portál pro všechny zaměstnance, který se plánuje doplnit informační brožurkou pro zaměstnance s upozorněním na relevantní rizika, postupy a chování v případě hrozby vzniku či vzniku krizových situací a dalších informací).

Cílem ochrany KI je zajistit přijatelnou míru jeho bezpečnosti a odolnosti, posilování vzájemné spolupráce a rozvoj povědomí za účelem efektivního řešení a zvládání případů selhání či narušení KI.

Efektivními postupy daný subjekt KI **významně podporuje a inspiruje další subjekty** a **posiluje tak celkovou připravenost státu** na řešení krizových situací. Nadto pozitivním efektem bylo též posílení významu ochrany KI a samostatné bezpečnosti z pohledu jeho vedení.

Zájem o danou problematiku vzrostl díky zapojení všech vedoucích zaměstnanců do krizového řízení, určení odpovědnostních vazeb a také **zintenzivnění komunikace a spolupráce** mezi organizačními útvary.

6. VÝSTUPY STUDIE

Případová studie předkládá podnětný příklad a prokazuje, že systémové postupy nejlepší praxe **lze implementovat i do řízení subjektu KI z veřejného sektoru** se zdánlivě nevýznamným postavením v oblasti řízení bezpečnosti státu.

Klíčové realizované systémové postupy a opatření při zavedení nového konceptu ochrany KI v podmínkách subjektu průzkumu:
- formulace a realizace strategie ochrany KI, cílená koordinace všech procesů;
- spolupráce na všech úrovních řízení i vně subjektu, pravidelné porady, vyžadování a vnímání zpětné vazby, neustálé hodnocení realizovatelnosti opatření v praxi, otevřená komunikace;
- zapojení všech zainteresovaných aktérů, klíčových zaměstnanců na všech úrovních řízení;
- jednotná a věcná plánovací dokumentace napříč úrovněmi řízení, založená na typových postupech (operativních kartách);
- vlastní systém řízení rizik krizových situací provázaný s řízením rizik;
- metodická podpora systémové proškolování, pravidelné porady, cvičení za účelem zvýšení připravenosti.

Možná **úskalí procesu zavádění**:
- omezená personální kapacita;
- časová náročnost postupných kroků, častá zpoždění při realizaci dílčích kroků vlivem nutnosti plnění úkolů jiných agend;
- nepochopení a podceňování ochrany KI ze strany některých vedoucích zaměstnanců;
- náročnost koordinace činností a sjednocení postupů všech pracovišť.

Srovnání situace před a po realizaci systémových opatření nabízí hodnotné výsledky. Některé dílčí kroky, jako je například realizace řízení kontinuity, jsou neustále předmětem zájmu a v budoucnosti budou realizovány. Proces tedy nelze uzavřít, ani striktně konstatovat, v čem byl neúspěšný.

Hlavním zjištěním je tak ověření skutečnosti, že zefektivnění a rozvoj ochrany KI v případě konkrétního subjektu KI z veřejného sektoru nejsou nedosažitelné, tj. jsou reálné.

7. DISKUSE

Ilustraci na jediném případu není sice možné považovat za objektivní z hlediska posuzování všech subjektů KI z veřejného sektoru, přesto u některých **lze usuzovat** na **podobnost situace a podmínek**, a tedy **i možný úspěch** při realizaci obdobného projektu.

Studie předkládá reálný případ, který nemusí být zčásti či zcela v praxi ojedinělý. Omezení však představují primárně konkrétní zázemí, kdy by výsledky patrně byly odlišné a nikoliv tak úspěšná v případě, že by byla realizována v prostředí, které by nereagovalo natolik pozitivně na zamýšlené změny. Přínosem byla podpora vedení, fungující vnitřní a vnější spolupráce, časové možnosti a zájem a odhodlání odpovědných pracovníků zlepšit stávající situaci.

Zkreslující mohou být některé prezentované výstupy co do jejich **snadnosti provedení**. Naopak, nešlo (nejde) o jednoduchý proces, nýbrž komplexní změnu, která vyžaduje mnoho času, proaktivní přístup, trpělivost, neustálou komunikaci a spolupráci. V tomto se může stát realizace obdobného procesu limitující a nesnadnou.

Metoda **zúčastněného otevřeného pozorování** se může negativně projevit v kvalitě výsledků. V realizovaném případě pozorovatelka byla zároveň zaměstnankyní organizace a pozorování tak bylo realizováno v rámci její pracovní činnosti. Do jisté míry šlo o pozorování vlastní činnosti pozorovatelky, kde je možnost ovlivnění kvality minimální, naopak spíše bylo motivací dosáhnout vytyčených cílů zvýšení ochrany KI.

Získané výstupy mají **další výzkumný potenciál**. Na jejich základě lze provést

následné kvantitativní, popř. i kvalitativní šetření s cílem zjistit konkrétní možnosti i u jiných subjektů KI z odvětví Veřejná správa či obecně z veřejného sektoru, popř. i srovnání se sektorem soukromým.

Následné kvalitativní šetření by mohlo spočívat také v další případové studii v podmínkách jiného subjektu KI. Výstupy případových studií by poté bylo možné komparovat a formulovat konkrétní doporučení k zavádění, resp. změnám přístupu k ochraně KI.

ZÁVĚR

V návaznosti na provedený průzkum a jeho výstupy lze konstatovat, že **prokazatelně jako nejlepší cesta k dosažení rozvoje ochrany KI je systémový přístup**.

Článek nadto prezentuje paletu možných postupů či opatření systémového charakteru, které jsou realizovatelné s předpokladem dosažení úspěchu u konkrétního subjektu KI z veřejného sektoru.

LITERATÚRA

[1] HENDL, J. *Úvod do kvalitativního výzkumu*. Praha: Karolinum, 1999. 277 s. ISBN 80-246-0030-7.
[2] LOUČKOVÁ, I. *Integrovaný přístup v sociálně vědním výzkumu*. 1. vyd. Praha: Sociologické nakladatelství (SLON), 2010. 311 s. ISBN 978-80-86429-79-3.
[3] *Metodika zpracování plánů krizové připravenosti podle § 17 až 18 nařízení vlády č. 462/2000 Sb.* [online]. [B.m.]: Ministerstvo vnitra – Generální ředitelství HZS ČR, 2011. [cit. 1.3.2017]. Dostupné z: http://www.hzscr.cz/soubor/metodika-zpracovani-pkp-2011-pdf.aspx.
[4] Nařízení vlády č. 462/2000 Sb., *k provedení § 27 odst. 8 a § 28 odst. 5 zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon)* v posledním znění.
[5] PUNCH, K. *Úspěšný návrh výzkumu*. 1. vyd. Praha: Portál, 2008. 230 s. ISBN 978-80-7367-468-7.
[6] ŠVAŘÍČEK, R. a kol. *Kvalitativní výzkum v pedagogických vědách*. 1. vyd. Praha: Portál, 2007. 377 s. ISBN 978-80-7367-313-0.
[7] Usnesení vlády ze dne 14. prosince 2011 č. 934 *k určení prvků kritické infrastruktury, jejichž provozovatelem je organizační složka státu* v posledním znění.
[8] YIN, R. K. *Case study research: design and methods*. 3rd ed. Thousand Oaks: Sage, 2003. xvi, 181 s. ISBN 0-7619-2552-X.
[9] Zákon č. 240/2000 Sb., *o krizovém řízení a o změně některých zákonů* v posledním znění.
[10] Zákon č. 412/2005 Sb., *o ochraně utajovaných informací a bezpečnostní způsobilosti* v posledním znění.
[11] KOPECKÝ, Z., ŠPAČEK. M. *Business Continuity Plan in Entities of Critical Infrastructure*. Krízový manažment. Žilina: Žilinská univerzita v Žilině. Fakulta bezpečnostného inžinierstva, 2017, 1/2017. ISSN:1336 – 0019.