

Posúdenie rizika v sektoroch kritickej infraštruktúry SR

Obsah

Úvod	2
1 Metodika posúdenia rizík v sektoroch kritickej infraštruktúry	3
1.1 Metodológia posudzovania rizík	3
1.2 Prípravná fáza	4
1.3 Realizačná fáza	5
1.3.1 Identifikácia hrozieb pre sektory KI	5
1.3.2 Hodnotenie vplyvu narušenia základnej služby hrozbami	12
1.3.3 Výsledné porovnanie sektorov kritickej infraštruktúry a interpretácia výsledkov	15
Reflexia za interpretáciu výsledkov	18
Odporúčané opatrenia na zvýšenie odolnosti kritických subjektov	20
Záver MV SR	23

Úvod

Pochopiť vzťah medzi rizikom a odolnosťou je kľúčové pre kontinuálne poskytovanie základných služieb podľa zákona č. 367/2024 Z. z. o kritickej infraštruktúre (ďalej zákon o KI). Posudzovanie rizík poskytuje informácie o kľúčových hrozbách, ich pravdepodobnosti a vplyve, čo je nevyhnutným predpokladom pre identifikáciu zraniteľných miest a návrh stratégie odolnosti. Na druhej strane, prístupy založené na odolnosti rozširujú tradičné posudzovanie rizík tým, že sa zameriavajú na schopnosť systému absorbovať narušenia, udržať si základné funkcie a obnoviť svoju funkčnosť.

Budovanie odolnosti si vyžaduje, aby sme mali kritický pohľad a dokázali objektívne pozrieť na vlastné zraniteľnosti a nedostatky. Musíme brať do úvahy najhoršie scenáre, ktoré zefektívňujú prevenciu, zvyšujú našu pripravenosť, a tým aj odolnosť¹.

Zvýšenie našej pripravenosti a pohotovosti na novú úroveň bude zároveň formovať, prispôsobovať a znižovať faktory, ktoré viedli k incidentom a krízam. Toto môže prispieť k odstráneniu potenciálnych agresorov a zároveň podporiť mitigáciu rozsahu a vplyvu klimatických zmien. Správne, účinne a trvalo udržateľne vykonaná príprava na celý rozsah možných hrozieb posilní budovanie odolnosti a bude obsahovať aj silný preventívny a rovnako aj zmierňujúci účinok.

Nestačí len reagovať na krízy, keď k nim dôjde, je potrebné byť pripravený. Základom je zvýšiť naše povedomie, mať komplexný obraz o hrozbách, ktoré sa vyvíjajú, a zabezpečiť, aby naše nástroje a spôsobilosti boli na túto úlohu dostatočne pripravené.

Komplexný súbor opatrení, ktoré sú podrobne opísané v stratégii, pomôže vytvoriť celkovú odolnosť na úseku kritickej infraštruktúry, ktorá bude schopná predvídať vlastné bezpečnostné potreby, plánovať ich a starať sa o ne, ktorá dokáže účinne reagovať na hrozby svoje základné služby a ktorá chráni potreby spoločnosti a demokracie².

Integrovaný prístup založený na všetkých zdrojoch hrozieb, ktorý pokrýva celé spektrum prírodno - klimatických, antropogénnych a hybridných hrozieb, poukazuje na skutočnú pripravenosť. Stratégia pripravenosti EÚ poukazuje prístup, ktorý podporuje koreláciu pripravenosti a odolnosti, do ktorej sú zapojené komunity a občianska spoločnosť, podniky a sociálni partneri, ako aj vedecká a akademická obec. Jeho cieľom je komplexne riešiť kľúčové riziká, ktoré vyplývajú z hrozieb, ich vzájomné pôsobenie a kaskádové účinky.

Posudzovanie rizík a ich riadenie musí byť neoddeliteľnou súčasťou každého subjektu, a to ako v horizontálnej, tak aj vo vertikálnej rovine verejnej správy. Tím Katedry krízového manažmentu na Žilinskej univerzite v Žiline, v spolupráci so SKR MV SR, vytvoril základné predpoklady na vývoj efektívneho interaktívneho nástroja a analytického dokumentu na posúdenie rizík v sektoroch kritickej infraštruktúry. Toto posúdenie identifikovalo základné služby ústredných orgánov na úseku KI, ktoré majú v súčasnom svete najzásadnejší vplyv na odolnosť SR. Cieľom je vytvoriť holistický prístup, ktorý kombinuje tradičné techniky posúdenia rizík s prvkami odolnosti. To znamená prechod od reaktívneho prístupu k

¹ Safer Together Strengthening Europe's Civilian and Military Preparedness and Readiness.

² ProtectEU: Európska stratégia vnútornej bezpečnosti.

proaktívnemu zameraniu na budovanie schopností, ktoré umožnia kritickým subjektom úspešne čeliť³.

Pri posudzovaní rizík sa postupuje podľa čl. 32 všeobecného nariadenia o ochrane údajov - GDPR, § 39 až 41 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, § 13 až 16 zákona 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a ustanovení aktu o umelej inteligencii.

1 Metodika posúdenia rizík v sektoroch kritickej infraštruktúry

Na základe dlhoročných vedecko-výskumných a projektových skúseností tímu KKM FBI UNIZA, dostupných probabilistických a deterministických postupov na Slovensku a v zahraničí, výsledkov dizertačných a habilitačných prác, medzinárodných vedeckých projektov a projektov riešených v schéme Horizon Europe, existujúcich manažérskych prístupov a noriem, a skúseností zo zahraničných bilaterálnych rokovaní v rámci EÚ a vo svete, sme vytvorili túto metodiku, interaktívny nástroj a analytický nástroj pre posudzovanie rizík v sektoroch KI. Pri ich tvorbe sme sa v úvode inšpirovali metódou hodnotenia a výberu na základe kritérií z existujúcich postupov, dobrej praxe a vlastných expertných skúseností. Tento prístup zaručuje objektívnosť, transparentnosť a opakovateľnosť posudzovacieho procesu, ktorý zohľadňuje viacero faktorov naraz. Postupy uvedené v metodike boli implementované do nového Interaktívneho dokumentu pre ústredný orgán, v ktorého pôsobnosti je základná služba (ďalej iba ústredný orgán) a Analytického nástroja (pre MV SR potrebného na vyhodnocovanie údajov z 10 interaktívnych nástrojov). Po zhodnotení rôznych prístupov bolo prijaté rozhodnutie pre kombináciu probabilistického a deterministického posudzovania rizík založené na "multi-hazard" analýze s využitím kritérií K1 - K6 a oblastí O1 - O5 pozostávajúcich z ďalších pod-kritérií potrebných na posúdenie vplyvu hrozieb na základnú službu.

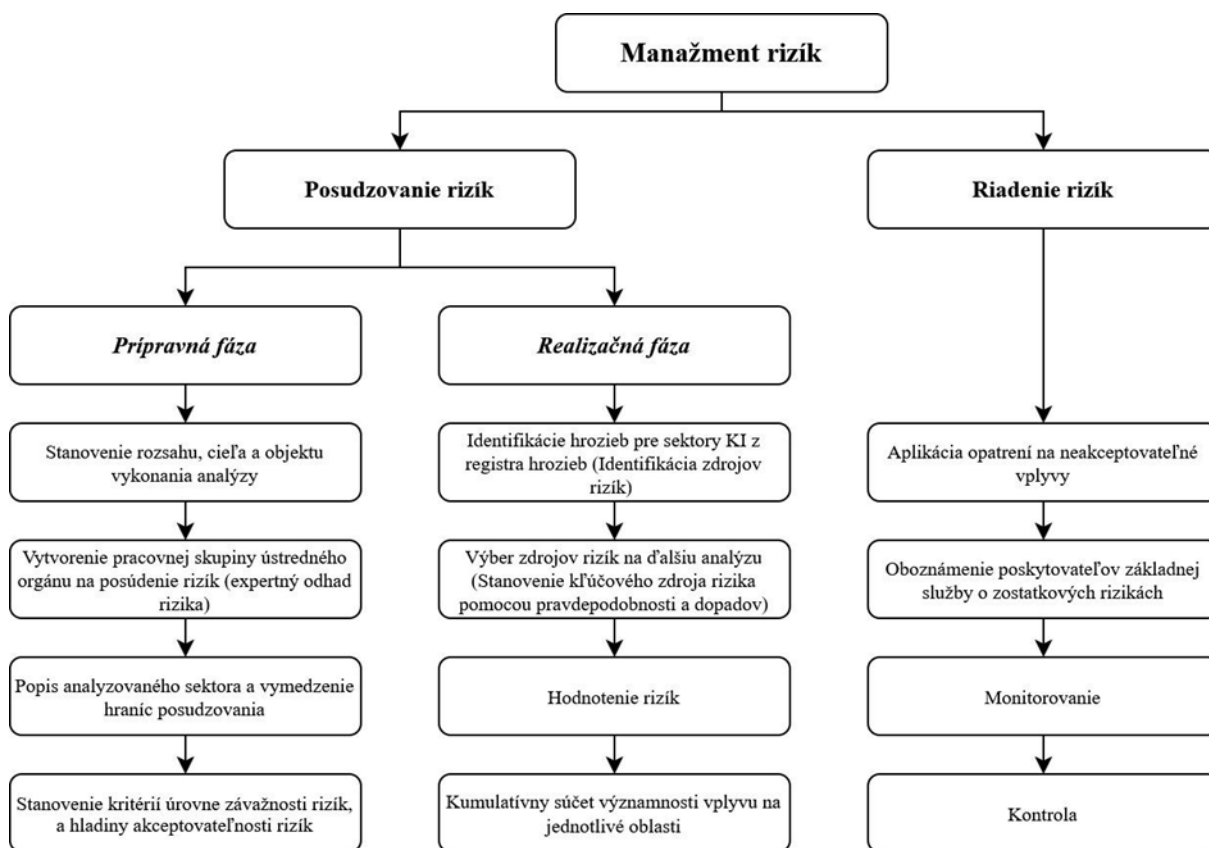
Deterministické posudzovanie je preferované, keď nie sú dostupné dostatočné alebo kvalitné štatistické údaje potrebné na odhad pravdepodobnosti. Deterministický prístup ponúka stabilnejšie hodnotenie oblastí O1-O5. Aj keď je možné použiť rôzne metódy a prístupy na posúdenie rizík, KKM FBI UNIZA a SKR MV SR sa rozhodli pre Multi-Criteria Decision Analysis (MCDA) s cieľom posúdiť základné služby a ich dopad na sektory KI. Dôležitým krokom bolo vytvorenie scenárov najhorších možných udalostí (ďalej WCS) v spolupráci s ústrednými orgánmi a SKR MV SR. Tieto scenáre umožnili podrobnejšie posúdiť jednotlivé hrozby a vytvoriť základ pre následné posudzovanie rizík. Posúdenie rizika v sektoroch KI vytvára predpoklad na zvyšovanie pripravenosti subjektov poskytujúcich základné služby rovnako ako ústredných orgánov. Týmto spôsobom sa postupne posilňuje ich odolnosť a znižuje zraniteľnosť voči mimoriadnym udalostiam a iným závažným hrozbám.

Z hľadiska celkovej prehľadnosti a úspory textu v dokumente uvádzame právne predpisy vstupujúce do posúdenia rizika, terminológiu na úseku KI a podrobný zoznam použitých zdrojov na tomto odkaze.

1.1 Metodológia posudzovania rizík

³ Ministerstvo vnútra Slovenskej republiky. Ochrana kritickej infraštruktúry [online]. Dostupné na: https://www.minv.sk/?Ochrana_kritickej_infrastruktury_1.

Táto podkapitola predstavuje metodologický rámec a postupy používané pri posudzovaní rizík vhodné pre kritickú infraštruktúru. Zameriava sa na systematické hodnotenie potenciálnych hrozieb a určenie opatrení na minimalizáciu ich dopadov na základnú službu. Obrázok 1 zobrazuje vývojový diagram, ktorý popisuje postup manažmentu rizík v sektoroch KI, ktoré má realizovať každý ústredný orgán a delí sa na posudzovanie a riadenie rizík.



Obr. 1 Komplexný model posúdenia rizika v sektoroch kritickej infraštruktúry

Posudzovanie rizík sa delí na prípravnú a realizačnú fázu, ktoré budú ďalej popísané a aplikované na prostredie KI.

1.2 Prípravná fáza

Prípravná fáza posudzovania rizík v sektoroch KI má charakter rozhodnutí a na to nadväzujúcich prípravných činností, ktorých vybrané výstupy sú prepojené s jednotlivými krokmi realizačnej fázy posudzovania rizík pre ústredný orgán.

Skladá sa z týchto krokov:

- **Stanovenie rozsahu, cieľa a objektu vykonania analýzy** - je potrebné si určiť, do akej hĺbky bude analýza vykonaná, čo závisí od viacerých faktorov. V prvom rade sa odvíja od účelu vykonávanej analýzy, ktorá má v tomto prípade charakter plnenia zákonných požiadaviek podľa zákona o KI, kde sa posúdenie rizika vykonáva podľa potreby, najmenej však raz za štyri roky. Zámerom posúdenia rizík podľa tejto metodiky je identifikovať vplyv hrozieb na poskytovanie jednotlivých základných služieb v sektoroch kritickej infraštruktúry, čím sa vytvoria predpoklady *pre prahové hodnoty významnosti vplyvu* podľa § 14 ods. 3 oznamovanie incidentov a významnosť vplyvu na poskytovanie základnej služby zákona o KI, *prahové hodnoty incidentov* podľa § 8 ods.

3 písm. E zákona o KI, *opatrení na zabezpečenie odolnosti kritických subjektov podľa § 10 zákona o KI.*

- **Vytvorenie pracovnej skupiny ústredného orgánu na posúdenie rizík (expertný odhad rizika)** - pracovná skupina a jej tvorba je v gescii každého ústredného orgánu samostatne. Vytvorenie pracovnej skupiny je individuálna záležitosť, ktorá sa odlišuje podľa cieľa, rozsahu a objektu vykonania analýzy a jej celkovej hĺbky. Kvalita vytvorenia pracovnej skupiny je priamo úmerná kvalite vykonania posúdenia rizík a presnosti expertného odhadu ústredného orgánu. Odporúča sa mať nepárny počet členov, kvôli prípadnému hlasovaniu v prípade nezhody v rozhodovaní (min.3 osoby).
- **Popis analyzovaného subjektu/základnej služby/podsektora/sektora a vymedzenie hraníc posudzovania** - podľa prílohy č.1 zákona o KI sa posudzuje každá základná služba samostatne, pričom sa skúma výsledný vplyv na sektory v pôsobnosti všetkých ústredných orgánov. V prípade určenia vplyvu základnej služby je možné identifikovať kategórie subjektov, ktoré majú najrušivejší vplyv na základnú službu v prípade vzniku incidentu v zmysle identifikovaných hrozieb.
- **Stanovenie kritérií úrovne závažnosti rizík, scenárov a hladiny akceptovateľnosti rizík** - Stanovenie jednotlivých úrovní akceptovateľnosti rizík pre všetky základné služby, identifikácia zraniteľností voči incidentom s nežiaducim vplyvom medzisektorovo a cezhranične, a rozvinutie najhorších scenárov a modelov hrozieb pre prípadné ďalšie využitie.

1.3 Realizačná fáza

Vzhľadom na kombináciu probabilistického a deterministického posúdenia rizík sme v realizačnej fáze hodnotili vplyv hrozieb na základnú službu ústredných orgánov, a akým spôsobom a či tento incident má vplyv na stanovené oblasti. Skladá sa z niekoľkých krokov, ktoré sú uvedené v ďalšom texte.

1.3.1 Identifikácia hrozieb pre sektory KI

V tomto prvom kroku realizačnej fázy sa jedná sa o proces hľadania, rozpoznávania a popisovania rôznych typov hrozieb. Významnú úlohu tu zohráva spolupráca so všetkými dotknutými rezortmi a subjektmi, pričom cieľom bolo vygenerovať podrobný register hrozieb. Dôležité je zdôrazniť, že iba identifikované hrozby budú ďalej analyzované a hodnotené. Pri posúdení rizík je potrebné vziať do úvahy jednotlivé sektorové asymetrie. Odporúčame preto identifikované hrozby, vyhodnotené ako menej rizikové tzn. “nepovinné” hodnotiť na základe dobrovoľnosti s prihliadnutím na sektorové odlišnosti a prípadne asymetrie.

Analýza rizík tvorí základ pre hodnotenie rizika. Riziko je vnímané ako pravdepodobnosť vzniku nežiaduceho účinku, ku ktorému dôjde počas určitej doby alebo za určitých okolností, pričom riziko je vždy spojené s konkrétnym typom zdroja rizika s konkrétnou hrozbou.

Predmetná analýza sa zameriavala na hodnotenie typov hrozieb evidovaných v registri hrozieb s cieľom identifikovať tie, ktoré majú priamy vplyv na poskytovanie základnej služby. Metodika analýzy využívala jednoduchú maticu rizík, ktorá slúži na systematické posúdenie pravdepodobnosti výskytu a potenciálneho dopadu každej identifikovanej hrozby. Zmyslom tohto procesu bolo selektovať hrozby na kľúčové a povinné, t. j. tie, ktoré majú vplyv na kontinuitu a kvalitu poskytovanej základnej služby.

Stanovenie rizík vychádzalo z nasledujúcich dokumentov, na základe ktorých bol vytvorený nový zoznam hrozieb v súčinnosti so všetkými ústrednými orgánmi štátnej správy:

- Register hrozieb Slovenskej republiky 2020 v kontexte civilnej ochrany obyvateľstva (aktualizácia 2022),
- Verejný referenčný katalóg hrozieb NBÚ pre prevádzkovateľov základných služieb podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti,
- Metodika vykonania prieskumu realizácie opatrení vyplývajúcich z hĺbkovej analýzy zraniteľností vybraných orgánov štátnej správy voči hybridným hrozbám (2023),
- Bezpečnostná stratégia Slovenskej republiky (2021)
- Prehľad zdrojov rizík a ohrození nevojenského charakteru (2014).

Východiskovými dokumentmi pre identifikáciu hrozieb sú;

- Národná stratégia riadenia rizík bezpečnostných hrozieb SR (uznesenie vlády SR č. 65/2022)⁴
- Metodika analýzy rizík kybernetickej bezpečnosti, NBÚ 6 (2021)⁵
- Metodika vykonania prieskumu realizácie opatrení vyplývajúcich z hĺbkovej analýzy zraniteľností vybraných orgánov ŠS voči hybridným hrozbám (2024)⁶
- Posúdenie rizík SR v súlade s článkom 6 Rozhodnutia Európskeho parlamentu a Rady č. 1313/2013/EÚ zo 17. decembra 2013 o mechanizme Únie v oblasti civilnej ochrany⁷
- Prehľad zdrojov rizík a ohrození nevojenského charakteru (2014)⁸

Tieto dokumenty predstavujú komplexný prístup k identifikácii, hodnoteniu a znižovaniu potenciálnych rizík, ktoré môžu ohroziť bezpečnosť a ochranu životných záujmov SR.

Na tvorbu zoznamu bola využitá Delphi metóda, ktorá umožnila dosiahnuť konsenzus odborníkov z rôznych rezortov pri identifikácii a prioritizácii hrozieb. Výsledný zoznam hrozieb bol rozdelený na povinné a nepovinné hrozby, ktoré sú zobrazené v tabuľke 1. Ku každej hrozbe bol priradený gestor a spolugestor riadenia rizika. Podstatnou časťou pre vykonanie selekcie hrozieb bolo správne nastavenie hodnotení, podľa ktorých sa posudzuje závažnosť rizika. Tieto výsledky boli dôležité pre určenie, či je hrozba významná alebo nie z hľadiska poskytovania základnej služby podľa prílohy č. I zákona č. 367/2024 Z. z. Na základe expertných participatívnych metód boli stanovené limitné hodnoty úrovni rizík. Pre každý typ hroby sa riziko určuje kombináciou pravdepodobnosti výskytu hrozby (P) a dopadu na prostredie SR (D) podľa vzorca:

$$R = P \times D$$

⁴ Uznesenie vlády Slovenskej republiky č. 280/2023 k Akčnému plánu k Národnej stratégii riadenia rizík bezpečnostných hrozieb SR do roku 2025.

⁵ Národný bezpečnostný úrad. 2021. Metodika analýzy rizík pre uplatnenie v procesoch riadenia rizika v zmysle požiadaviek zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti [online]. Dostupné na: https://www.nbu.gov.sk/wp-content/uploads/2021/12/Metodika_analyza_rizik_v1.0_12_2021.pdf.

⁶ Ministerstvo vnútra Slovenskej republiky. Interný dokument.

⁷ Ministerstvo vnútra Slovenskej republiky, Sekcia krízového riadenia. Analýza územia z hľadiska možných mimoriadnych udalostí jednotlivých regiónov Slovenskej republiky: podľa zákona č. 42/1994 Z. z. a pokynu č. SKR-OIZS-2013/000403-1, ktorým sa upravuje štruktúra a obsah dokumentu „Analýza územia z hľadiska možných mimoriadnych udalostí“. Interný dokument.

⁸ Ministerstvo obrany Slovenskej republiky. Interný dokument.

Tab. 1 Zoznam hrozieb

Názov hrozby		
Naturogénne hrozby - B - Biotické		
Kód	Povinné	Nepovinné
B01	hromadná nákaza osôb (epidémia)	
B02	hromadná nákaza živočíchov (epizootia)	
B03	hromadná nákaza rastlín	
B04		zamorenie hmyzom
Naturogénne hrozby - A - Abiotické		
Kód	Povinné	Nepovinné
A01	povodeň/prívalové dažde	
A02		snehová kalamita
A03		krupobitie
A04		poľadovica a námraza
A05	extrémny vietor	
A06		tornádo
A07		extrémne nízka teplota
A08	extrémne vysoká teplota	
A09		atmosférické výboje
A10	dlhodobé sucho	
A11	svahový zosuv	
A12		snehová lavína
A13	zemetrasenie	
A14		vulkanická činnosť
A15	požiar	
Naturogénne hrozby - K - Kozmické		
Kód	Povinné	Nepovinné

K01		impakt mimozemského telesa
K02		meteorický dážď
K03		solárna búrka
K04		extrémne kozmické žiarenie
K05		pád umelého kozmického zariadenia
Antropogénne hrozby - T - Technogénne		
Kód	Povinné	Nepovinné
T01	únik nebezpečnej chemickej látky zo stacionárneho zariadenia vrátane produktovodov	
T02		únik nebezpečnej chemickej látky
T03		únik biologických agens
T04	radiačná havária a únik radiačnej látky	
T05		výbuch v sklade výbušnín, trhavín, munície a streliva
T06		nález nevybuchnutej munície
T07		výbuch a požiar v zástavbe a priemysle s výnimkou stacionárnych zdrojov NL
T08	environmentálna záťaž	
T09		závažná nehoda v cestnej doprave
T10		závažná nehoda v leteckej doprave
T11		závažná nehoda vo vnútrozemskej vodnej doprave
T12		závažná nehoda v železničnej doprave
T13	narušenie dodávok elektrickej energie veľkého rozsahu	
T14	narušenie dodávok plynu veľkého rozsahu	

T15	narušenie dodávok pitnej vody veľkého rozsahu	
T16	narušenie dodávok potravín veľkého rozsahu	
T17		narušenie dodávok tepla veľkého rozsahu
T18	narušenie dodávok ropy a ropných produktov veľkého rozsahu	
T19	rozrušenie vodných stavieb	
T20		narušenie plynulosti poštového prepravného reťazca
T21	narušenie elektronických komunikačných sietí	
T22	narušenie bezpečnosti informačných systémov a sietí vrátane kybernetických útokov	
Antropogénne hrozby - S - Sociogénne		
Kód	Povinné	Nepovinné
S01	migrácia veľkého rozsahu	
S02		narušenie poskytovania zdravotnej starostlivosti
S03		narušenie sociálneho systému
S04	narušenie poskytovania pomoci v tiesni	
S05	narušenie zákonosti veľkého rozsahu (porušovanie všeobecne záväzných právnych predpisov veľkého rozsahu) vrátane terorizmu	
S06		destabilizácia a narušenie chodu orgánov verejnej moci
S07		sociálne nepokoje veľkého rozsahu (rabovanie obchodov, skladov, hromadný útoky na majetok, atď.)

S08		etnické, náboženské a ideologické konflikty veľkého rozsahu
S09	ohrozenie, útok a sabotáž proti objektom osobitnej dôležitosti a ďalším dôležitým objektom	
S10		strata kontroly nad časťou, alebo celým územím Slovenskej republiky
S11	narušenie vzdušného priestoru (vrátane bezpilotných leteckých systémov)	
S12		aktivizmus s negatívnym vplyvom na prevádzkovanie základnej služby
Antropogénne hrozby - E - Ekonomické		
Kód	Povinné	Nepovinné
E01	narušenie menového, devízového a finančného hospodárstva štátu	
E02	ekonomické ovplyvňovanie treťou stranou - bezpečnostné riziko tretej strany vzhľadom na analýzu vlastníckej štruktúry a riadiacej štruktúry tretej strany vrátane vlastníckeho podielu cudzieho štátu a priamych zahraničných investícií do tretej strany	
E03	nedostatočná diverzifikácia dodávateľov kritických služieb a kritických komponentov alebo surovín	
Antropogénne hrozby - H - Hybridné		
Kód	Povinné	Nepovinné
H1	zhromažďovanie, vyhodnocovanie, spracovanie a šírenie informácií neoprávneným spôsobom, v neprospech štátneho zriadenia alebo kritického subjektu	

H2		hrozby vyplývajúce z informácií špecifických pre cudzí štát a informácie spravodajskej služby o možných hrozbách pre záujmy Slovenskej republiky
H3		strata slobody rozhodovania a konania na strategickom, operačnom a taktickom stupni štátu zo strany predstaviteľov verejnej moci
H4		znemožnenie presadzovania záujmov (národno-štátnych, organizačných) na medzinárodnej úrovni
H5		nátlak na politikov alebo vládu SR
H6	ovplyvňovanie kľúčových pracovníkov kritických subjektov	
H7		možnosť ovplyvňovania a zasahovania do činnosti tretej strany štátom, ktorý nie je členským štátom Európskej únie a Organizácie Severoatlantickej zmluvy
H8		úmyselné šírenie propagandy za účelom ovplyvňovania mienky v neprospech verejného záujmu (štátneho orgánu, organizácie)
H9	úmyselné zverejnenie informácií v neprospech verejného záujmu (štátneho orgánu, organizácie)	
H10	šírenie poplašných správ za účelom prerušenia poskytovania základnej služby	
H11		zneužívanie slabých miest, nejednoznačností a medzier v legislatíve
H12		ovládanie a zasahovanie do médií
H13		podpora a využívanie korupcie

H14		spravodajské (utajené) operácie a infiltrácia (prezradenie chránených záujmov)
H15		využívanie slabých miest vo verejnej správe

Každá hrozba, zaznamenaná v registri, bola zo strany gestora riadenia rizika podrobená detailnému modelovaniu. Toto modelovanie spočívalo v špecifikácii najhoršieho možného scenára, ktorý predstavuje najkritickejší priebeh realizácie danej hrozby. Následne sa na základe tohto scenára posudzovali kritéria (K1-K6) a oblasti vplyvu (O1-5) na jednotlivé základné služby. Cieľom je pochopiť nielen samotnú hrozbu, ale aj jej potenciálne následky v najnepriaznivejšej situácii, čo umožňuje efektívnejšie nastavenie priorít a alokáciu zdrojov na zmiernenie rizík.

Vzhľadom na inherentnú asymetriu sektorov kritickej infraštruktúry, ústredný orgán disponuje možnosťou voľiteľne pridávať tzv. nepovinné hrozby medzi svoje povinné riziká. Toto rozhodnutie je plne v kompetencii ústredného orgánu a odvíja sa od povahy jeho základnej služby a špecifických rizík, ktorým môže základná služba vystavená. Táto flexibilita umožňuje prispôbiť posúdenie rizík individuálnym potrebám a kontextu každého sektora. Výsledkom tejto analýzy by mala byť jasná identifikácia povinných a nepovinných hrozieb, ktoré priamo ohrozujú schopnosť subjektu poskytovať základnú službu.

1.3.2 Hodnotenie vplyvu narušenia základnej služby hrozbami

Pri stanovení významnosti vplyvu sa posudzuje jeho dopad na jednotlivé oblasti a rozsah šírenia vplyvu v súlade s oznámenia a usmernenia Komisie, vzor na podávanie správ sa vypracuje podľa článku 5 ods. 5, článku 6 ods. 6 a článku 7 ods. 3 smernice (EÚ) 2022/2557 o odolnosti kritických subjektov. Významnosť vplyvu na poskytovanie základnej služby sa posudzuje podľa § 14 ods. 3 zákona č. 367/2024 Z. z. o kritickej infraštruktúre a o zmene a doplnení niektorých zákonov podľa kritérií, ktoré sú v tabuľke 2.

Tab. 2 Stanovené kritéria a charakteristika

Kritérium	Popis
K1	Počet užívateľov využívajúcich základnú službu, ktorú dotknutý subjekt poskytuje
K2	Miera, v akej iné sektory a podsektory uvedené v prílohe č. 1 zákona závisia od predmetnej základnej služby
K3	Trhový podiel subjektu na trhu s dotknutou základnou službou alebo dotknutými základnými službami
K4	Geografická oblasť, ktorú by incident mohol ovplyvniť, vrátane cezhraničného vplyvu, s prihliadnutím na zraniteľnosť určitých typov oblastí, ako sú vzdialené regióny alebo horské oblasti
K5	Význam subjektu z hľadiska zachovania dostatočnej úrovne poskytovania základnej služby, so zohľadnením dostupnosti alternatívnych spôsobov jej

	poskytovania
K6	Trvanie negatívneho dopadu na poskytovanie základnej služby

Kritériá K1 až K5 posudzujú závažnosť vplyvu, zatiaľ čo K6 hodnotí jeho trvanie. Z tohto dôvodu je potrebné ich spoločné hodnotenie pre každú z oblastí. Gestor ochrany základnej služby si stanovuje pre každú základnú službu znenie a prahové hodnoty jednotlivých kritérií individuálne, v súlade s § 6 písm. a) a b) zákona č. 367/2024 Z. z. a určuje pri nich hodnotu, kedy je to významný rušivý vplyv v súlade s § 9 písm. c) zákona č. 367/2024 Z. z. V prípade potreby môže byť každé kritérium ďalej rozdelené na podkritériá. Všetky kritériá (K1 až K6) musia byť hodnotené na škále od 1 do 5, pričom 1 predstavuje minimálnu (prípadne žiadnu) závažnosť a 5 najvyššiu (katastrofickú) úroveň závažnosti.

Posledným krokom posúdenia rizík je hodnotenie vplyvu, ktorý by mohli mať hrozby z hľadiska ich závažnosti a trvania na jednotlivé oblasti (O) tak ako to je zobrazené v tabuľke 3.

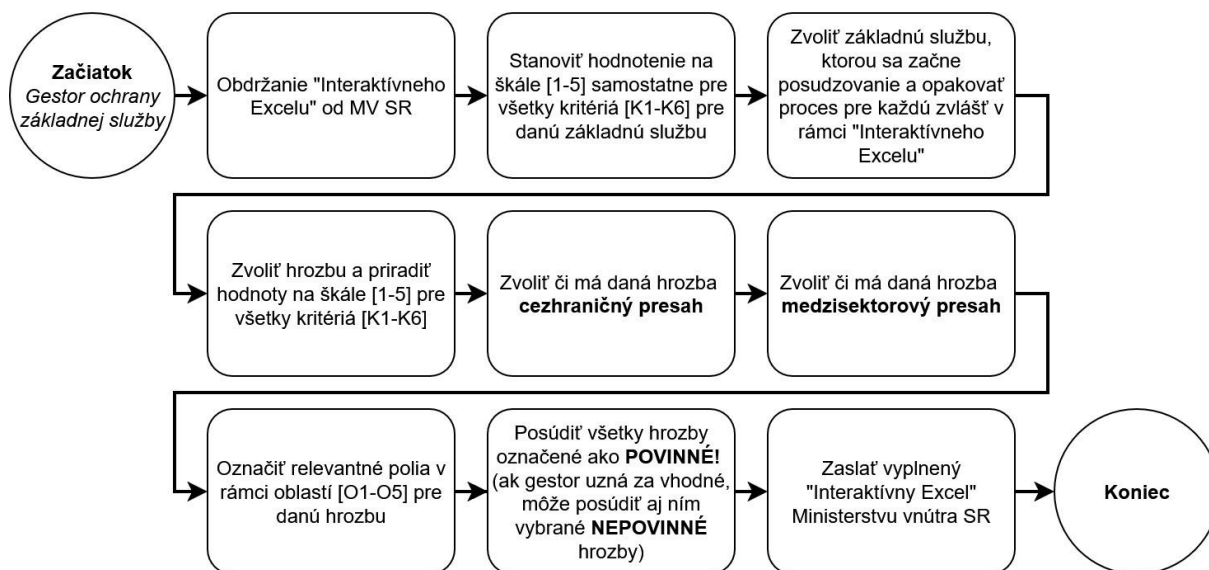
Tab. 3 Stanovené oblasti a charakteristika

Oblasť	Popis
O1	Hospodárska činnosť
O2	Spoločenská činnosť
O3	Životné prostredie
O4	Verejná ochrana a bezpečnosť
O5	Zdravie obyvateľstva

Jednotlivé oblasti sú hodnotené prostredníctvom podkritérií, ktoré reflektujú požiadavky smernice Európskeho parlamentu a Rady (EÚ) 2022/2557 (CER) a sú zaznamenané vo forme zaškrtnutých políčok (checkboxov). Na základe počtu označených podkritérií v rámci každej oblasti sa stanoví čiastková hodnota vplyvu na škále 1 – 5. Gestor ochrany základnej služby si môže stanoviť kvalitatívne hodnoty potrebné na označenie jednotlivých podkritérií. Zároveň stanovuje prahové hodnoty incidentov individuálne pre každú jeho základnú službu v súlade s § 8 ods. 3 písm. e) zákona č. 367/2024 Z. z. Ústredný orgán je povinný posúdiť hrozby, ktoré predstavujú neakceptovateľné riziko a zároveň môže podľa vlastného uváženia posúdiť aj hrozby s nižšou závažnosťou. V prípade, že nie je možné niektorú hrozbu objektívne posúdiť, môže využiť konzultácie s gestorom rizika, s ktorým spoločne prediskutujú možné negatívne dopady danej hrozby na poskytovanie základnej služby. Ústredný orgán samostatne posúdi relevantné hrozby vplývajúce na základnú službu, za ktorú zodpovedá. Ak identifikuje zraniteľnosť voči incidentom s nežiaducim vplyvom medzisektorovo, cezhranične označí to pri príslušnej hrozbe. Výsledný vplyv na jednotlivé oblasti, ako aj celkový vplyv na základnú službu, sa určí po vyhodnotení všetkých relevantných hrozieb. Zároveň sa určí prítomnosť nežiaduceho vplyvu na iný sektor a nežiadúceho cezhraničného vplyvu.

Na tvorbu vývojového diagramu postupnosti krokov pre vykonanie posúdenia rizika v sektoroch kritickej infraštruktúry sú využité diagramy tokov (flowcharts), ktoré vizuálne

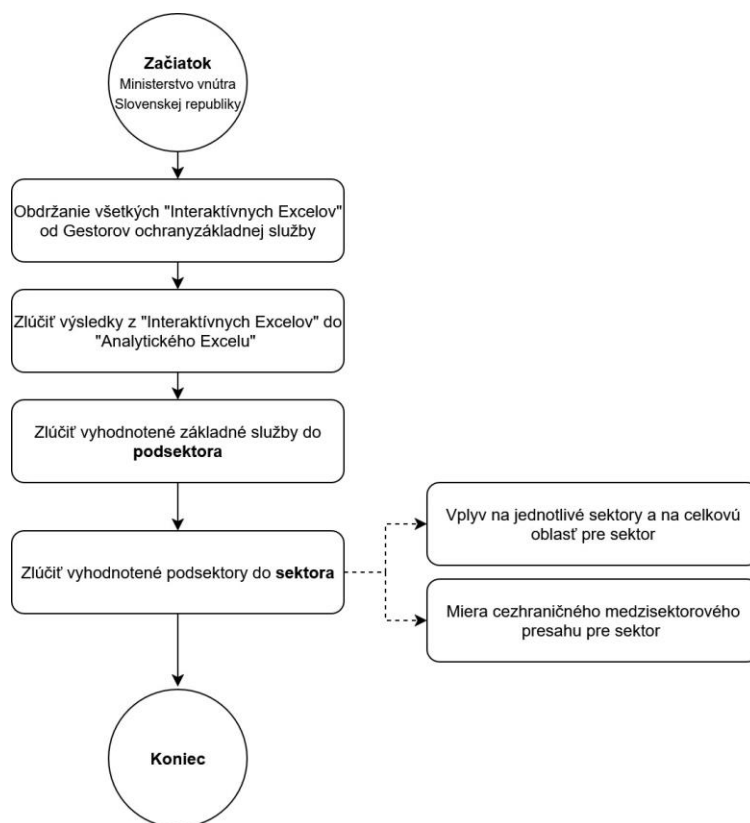
znázorňujú jednotlivé fázy procesu pre posudzovateľa za základnú službu v jeho pôsobnosti, ako je to zobrazené na obrázku 2.



Obr. 2 Proces hodnotenia v rámci posúdenia rizík pre potreby posúdenia základnej služby

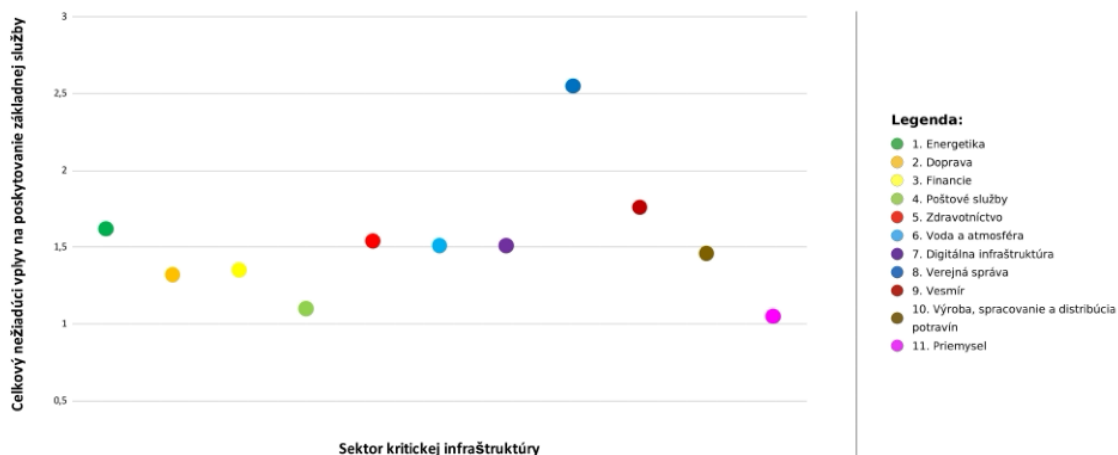
Výsledné hodnotenia vplyvu incidentov na poskytovanie základných služieb sa následne predkladajú MV SR.

Obrázok 3 znázorňuje vývojový diagram, ktorý predstavuje proces spracovania dát Ministerstvom vnútra SR v rámci posúdenia rizík v sektorech kritickej infraštruktúry SR. Proces začína získaním všetkých údajov z "Interaktívnych Excelov" od gestorov ochrany základnej služby, následne sa tieto údaje zlúčia do "Analytického Excelu". Výsledkom je získanie hodnotení, pričom sa každé delí do úrovni vyhodnotenia: vplyv na jednotlivé oblasti O1 až O5, celkovú oblasť pre sektor, miera cezhraničného a medzisektorového presahu pre sektor.



Obr. 3 Proces spracovania dát v rámci posúdenia rizík pre potreby MV SR

1.3.3 Výsledné porovnanie sektorov kritickej infraštruktúry a interpretácia výsledkov



Obr. 4 Výsledné porovnanie sektorov KI podľa výsledného vplyvu na všetky oblasti

Na základe realizačnej fázy probabilisticko-deterministického posúdenia rizík, ktorú vykonali ústredné orgány prostredníctvom špeciálne navrhnutých interaktívnych nástrojov zameraných na ich základné služby, boli výsledky zozbierané MV SR. Všetkých desať interaktívnych nástrojov bolo integrovaných do Analytického nástroja, ktorý zohľadňoval logiku posúdenia rizík v súlade so zákonom o KI a zároveň reflektoval logiku hodnotenia od základnej služby podľa tabuľky uvedenej v prílohe 1. Tento metodologický prístup umožnil objektívne a

konzistentné vyhodnotenie výsledkov posúdenia, ktorých prezentácia je znázornená na obrázku 4, kde sú uvedené výsledky presne tak, ako boli doručené od ústredných orgánov.

Výsledky posúdenia rizík v sektoroch kritickej infraštruktúry predstavujú dôležitý krok k zvyšovaniu odolnosti Slovenskej republiky v oblasti kritickej infraštruktúry. Z porovnávaných sektorov dosiahol najvyššie výsledky sektor „Verejná správa“. Tento sektor je tvorený iba jednou základnou službou, a to: „služby, ktoré poskytujú subjekty verejnej správy na úrovni ústrednej štátnej správy“. Nezastupiteľnosť predmetnej základnej služby pre štandardné fungovanie štátu a zároveň pre fungovanie viacerých ďalších základných služieb z iných sektorov spôsobila takýto významný výsledok. Uvedená základná služba a tým aj celý sektor, patrí do pôsobnosti MV SR. Dá sa preto predpokladať, že vzhľadom na jeho právne postavenie v zákone o KI budú výsledky ďalej detailne analyzované a na základe identifikovaných nedostatkov budú prijaté potrebné opatrenia na zvýšenie odolnosti daného sektora. Najmenej rizikový výsledok z porovnávaných sektorov dosiahol sektor „Priemysel“. Skutočnosť, že dosiahol najlepšie hodnotenie, však neznamená, že nie je potrebné prijímať ďalšie opatrenia na zvyšovanie jeho odolnosti. Pozitívne výsledky poukazujú na vysokú pripravenosť sektora a alternatívnosť zastúpenia subjektov, avšak zároveň zdôrazňujú potrebu pokračovať v nastavených trendoch a pravidelnejšie vykonávať samotné posúdenie. Iba tak možno zabezpečiť, aby v prípade pribudnutia nových subjektov alebo iných zmien nebola významne oslabená jeho aktuálna pozícia.

Ostatné hodnotené sektory dosiahli výsledky pohybujúce sa medzi uvedenými dvoma extrémami. V týchto prípadoch možno pozorovať rozdielnu úroveň pripravenosti, pričom jednotlivé sektory majú špecifické silné aj slabé miesta, s ktorými sa musia systematicky vysporiadať. Kým silné stránky umožňujú zabezpečovať kontinuitu základných služieb aj v náročnejších podmienkach, slabé miesta predstavujú potenciálne riziko, ktoré môže negatívne ovplyvniť ich stabilitu. Úlohou ústredných orgánov je preto zamerať sa na postupné odstraňovanie kritických miest prostredníctvom cielene prijímaných opatrení, ktoré budú reflektovať aktuálne hrozby aj budúce výzvy a posilňovanie silných miest. To umožní zabezpečiť dlhodobú odolnosť všetkých sektorov kritickej infraštruktúry a ich schopnosť efektívne fungovať aj v podmienkach krízových situácií. Výsledky posúdenia by mali poskytovať obraz o tom, kde sa jednotlivé sektory nachádzajú z hľadiska ich odolnosti voči rôznym hrozbám. Rovnako dôležité ako samotné porovnanie sektorov medzi sebou je skutočnosť, že každý ústredný orgán má presne stanovenú mieru odolnosti všetkých základných služieb vo svojej pôsobnosti, ako aj rozsah dopadu jednotlivých hrozieb na ich poskytovanie. Na základe výsledkov sa následne môže sústrediť na najvýznamnejšie nedostatky a v nadväznosti prijať opatrenia na zvýšenie pripravenosti čeliť hrozbám. To prispeje k stabilnejšiemu zabezpečovaniu základných služieb aj v prípade rôznych negatívnych okolností.

Vzhľadom na realizáciu prvého a rozsiahleho posúdenia rizika v rámci Slovenskej republiky je potrebné zohľadniť mieru subjektivity a neistoty vo výsledkoch. Analýza neistoty bola realizovaná na základe absencie posúdenia 7 základných služieb z objektívnych i subjektívnych dôvodov.

Pri kvantifikácii neistoty vychádzame z predpokladu, že tri zo základných služieb majú veľmi zásadný (vysoký) vplyv na výsledný hodnotiaci model. Ďalšia základná služba má stredný vplyv, ktorý je odvodený z jej prepojenia s ostatnými základnými službami. Zvyšné tri služby nemajú žiadny vplyv z dôvodu predpokladu, že ich poskytovanie nastane až v budúcnosti.

Vzhľadom k celkovému počtu 73 služieb sme využili jednoduché matematické modely na minimalizáciu neistoty a zvýšenie presnosti posúdenia rizík.

Pre stanovenie vplyvu nevyplnených služieb sme použili binomickú štatistickú metódu na výpočet intervalu spoľahlivosti podielu nevyplnených služieb, ktorá kvantifikuje neistotu spojenú s absenciou dát. Výpočet neistoty spôsobenej nevyplnenými službami ukazuje, že pravdepodobnosť, že tieto služby ovplyvnia výsledky, sa pohybuje v rozmedzí približne od 2,7 % do 16,5 %. Tento interval odráža mieru neistoty spôsobenú nedostatkom dát o siedmich chýbajúcich službách.

Druhá miera vplyvu na výsledky vychádza zo skutočnosti, že 50% ústredných orgánov nemalo pri posudzovaní adekvátnych odborníkov na procesy posúdenia rizík, ale mali odborníkov na oblasť KI. Podľa tendencií v určitých prípadoch je potrebné tento trend zohľadniť aj vzhľadom na to, že hrozby mohli byť v niekoľkých prípadoch podhodnotené. Na základe dostupných informácií a expertízy sme odhadli expertným odhadom, že 50 % hodnotení je ovplyvnených stredne významnými subjektívnymi faktormi, najmä z dôvodu chýbajúcej odbornej kvalifikovanosti pri posúdení rizík.

Reflexia za interpretáciu výsledkov

Všetky ústredné orgány verejnej správy vynaložili maximálne úsilie na vykonanie čo najkvalitnejšieho posúdenia rizík, pričom ich prístupy reflektovali dostupné metodológie a kompetencie v danom čase. Súčinnosť pri odbornom zhodnotení pri tomto procese poskytol ústredným orgánom tím odborníkov z KKM FBI UNIZA.

V úvodnej časti je však nutné zdôrazniť, že vykonané posúdenia rizík sa nezameriavajú na posúdenie samotných subjektov kritickej infraštruktúry, ale na analýzu vplyvu identifikovaných hrozieb na základné služby, ktoré sú v gescii ústredného orgánu.

V rámci výkonu týchto posúdení pôsobia na oddeleniach a v sekciách odborníci s potrebným technickým zázemím v oblasti kritickej infraštruktúry. Avšak, v niektorých prípadoch absentuje dostatočný rizikologický pohľad, ktorý by umožnil objektívnejšie a komplexnejšie zhodnotiť riziká. Vzhľadom na poddimenzované kapacity v mnohých oblastiach bezpečnosti a v kontexte súčasnej geopolitickej situácie je preto nevyhnutné reflektovať tieto aspekty vo vnútri expertnej komunity.

Avšak, je nevyhnutné zdôrazniť, že celoživotné vzdelávanie zostáva kľúčom k udržiavaniu tempa a aktuálnosti v tejto dynamickej a rýchlo sa meniacej oblasti, najmä v kontexte bezpečnostnej situácie v EÚ a globálne.

Ďalším odporúčaním, vychádzajúcim z praktických skúseností, je preferencia tímového prístupu pri vykonávaní posúdenia rizík založeného na expertnom hodnotení. Tento prístup je nielen časovo efektívnejší a umožňuje rýchlejšie spracovanie výsledkov, ale zároveň významne prispieva k zvýšeniu objektivity a zníženiu miery subjektivity v hodnotení. Ideálne je, aby na procese participovali minimálne tri osoby, pričom ich počet môže byť rozšírený na zvýšenie efektivity a kvality výsledného posúdenia.

V prípade dostatočného časového rámca je tiež žiaduce nadviazať úzku spoluprácu medzi gestormi riadenia rizík (hrozieb) a príslušnými ústrednými orgánmi, čo by mohlo ďalej zvýšiť presnosť a relevantnosť posúdenia.

Pri tvorbe Interaktívneho nástroja sme usilovali o dosiahnutie konsenzu medzi zainteresovanými stranami. Nástroj sa ukázal ako veľmi sofistikovaný pre niektorých používateľov, avšak niektorí by privítali začlenenie väčšieho počtu podkritérií na hodnotenie, čo by mohlo zvýšiť jeho presnosť a použiteľnosť.

V budúcnosti by metodika mohla obsahovať detailnejšie definované podkritériá, čo by umožnilo ešte precíznejšie posúdenie rizík. Tento proces však vyžaduje dôsledné hľadanie konsenzu, a na tento účel bude využitý aj štatistický dotazník, ktorý bude distribuovaný medzi relevantnými odborníkmi s cieľom zosúladiť očakávania a požiadavky na metodiku.

Odporúčame kritickým subjektom využiť tento dokument na samoposúdenie rizík po určitých úpravách a vytvorenie bezpečnostného plánu. Kritické subjekty by mali vykonávať posúdenie rizík na úrovni svojich prevádzok, zamerané na vplyv hrozieb na svoje základné služby. Tento proces si nie je možné zamieňať s posúdením hrozieb pre havarijné či bezpečnostné plány, ktoré však môžu tvoriť významné vstupy. Pri implementácii odporúčame konzultácie s ústrednými orgánmi a predstaviteľmi akademickej obce na zabezpečenie správnosti a aktuálnosti posúdení.

Ďalšie odporúčania:

- Zavedenie minimálnych bezpečnostných štandardov v rôznych sektoroch, ktoré budú mať odporúčací charakter.
- Každé nastavenie kritérií ústredného orgánu je kľúčovou činnosťou pred začatím posudzovania rizík a vyžaduje si medzirezortnú spoluprácu.
- Je potrebné riešiť poddimenzované stavy v štátnej správe a nedostatok odborníkov na posudzovanie rizík. Odporúča sa zapojiť odborníkov, akademickú obec a poskytovateľov.

Je dôležité zdôrazniť, že nie každá základná služba má priamy alebo rovnomerný vplyv na všetky definované oblasti (O1-O5). Tento vplyv sa odvíja od povahy samotnej základnej služby a od špecifických rizík, ktorým môže byť daný sektor vystavený. Ako bolo spomenuté vyššie (pri identifikácii hrozieb) *„vzhľadom na asymetriu sektorov kritickej infraštruktúry, kde jednotlivé sektory a ich základné služby majú odlišnú povahu a zraniteľnosť, má ústredný orgán možnosť tieto nepovinné hrozby “voliteľne” začleniť medzi svoje povinné hrozby. Toto rozhodnutie závisí od špecifickej povahy poskytovanej základnej služby a od relevantných rizík, ktorým je daný sektor vystavený.“*

Odporúčané opatrenia na zvýšenie odolnosti kritických subjektov

Opatrenia a činnosti založené na riziku sú jedným z kľúčových princípov subjektov a funkčnosti ich kritickej infraštruktúry. Znamená to, že akékoľvek opatrenia prijaté na zabezpečenie odolnosti kritickej infraštruktúry by mali byť úmerné veľkosti rizika narušenia fungovania základnej služby. To platí pre všetky sektory kritickej infraštruktúry, ich vzájomných závislostí, tak aj využitie zdrojov (aktív). Vzhľadom na dôležitosť tohto princípu v praxi funkčnosť prevádzky základnej služby a systémov kritickej infraštruktúry znamená prijať opatrenia na zníženie rizika narušenia kritickej infraštruktúry a uviesť odporúčania na stanovenie priorít ďalších činností.

Pred začatím akejkoľvek analýzy súvisiacej s rizikom (vplyv neistoty na stanovený cieľ alebo ciele) je potrebné mať na pamäti tri dôležité priority.

V prvom rade je potrebné mať na pamäti, že odhad rizika je komplexná oblasť, ktorý podľa ISO 31000⁹ pozostáva z nasledujúcich procesov:

- identifikácia hrozieb,
- analýza rizík,
- hodnotenie rizík.

V druhom rade Smernica CER v článku 4 upozorňuje na podstatu posúdenia rizík a úlohovo orientovanej spolupráce vyplývajúcej z úrovne vzájomných závislostí s koordinátormi iných systémov (medzisektorové závislosti a vzájomné závislosti). Pre kritické subjekty je posúdenie rizík a bezpečnosti kritickej infraštruktúry odporúčaním pre riadne riadenie organizácie, kde je verejná úloha chápaná ako súbor povinností a úloh, ktoré sa majú vykonávať, nemusí byť vždy zhodná s obchodnými cieľmi vyplývajúcimi z účasti jeho aktív v jednotnom zozname kritickej infraštruktúry (zariadení, inštalácií, vybavenia a služieb, ktoré tvoria kritickú infraštruktúru).

Po tretie, analýza hrozieb a posudzovanie rizík a následné riadenie rizík je cyklický proces vyplývajúci z nariadení, noriem, prevádzkových alebo kvalitatívnych režimov platných pre konkrétnu kritickú infraštruktúru, vedeckovýskumných poznatkov, ako na národnej tak i medzinárodnej úrovni, okrem bezpečnostnej politiky kritického subjektu alebo odporúčaní koordinátora systému kritickej infraštruktúry, ak boli prijaté a implementované.

Najlepším spoločným menovateľom pre vykonanie koherentného posúdenia rizík analýzy je teória riadenia kontinuity činnosti organizácie, alebo konkrétnejšie, jej idea potreby neprerušovaného vykonávania kritických procesov organizácie.

Veľmi dôkladná znalosť, pochopenie a popis špecifik činnosti organizácie, ako interne, tak aj externe, by mali byť prioritnou činnosťou, ktorá bezprostredne predchádza procesu odhadu rizík. To znamená vymenovať a systematizovať procesy vykonávané v organizácii. V praxi sa na tento účel najčastejšie odporúča vykonať takzvanú analýzu vplyvu na podnikanie (udalosť) (BIA – Business Impact Analysis), ktorej výsledkom je identifikácia kritických procesov.

⁹ ISO 31000 je prijatá do sústavy slovenských technických noriem prekladom ako STN ISO 31000 Manažérstvo rizika. Návod, ktorú odplatne poskytuje Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky prostredníctvom Portálu noriem.

Aby bolo možné efektívne a hodnotne odhadnúť riziko pre organizáciu, je potrebné vytvoriť správne podmienky pre celý proces nazývaný riadenie rizík. Norma ISO 31000 navrhuje vytvorenie tzv. rámcovej štruktúry riadenia, ktorá poskytuje základ a opatrenia, ktoré sa majú implementovať na každej úrovni organizácie. BIA by sa mala vykonávať pre každý proces implementovaný organizáciou, pričom sa zohľadňujú závislosti a vzťahy medzi rôznymi procesmi.

Výsledkom BIA by malo byť:

- posúdenie rizika spojeného s prerušením každého procesu,
- posúdenie finančných strát a strát reputácie spojených s akýmkoľvek prerušením procesu,
- odhad faktorov, ktoré môžu viesť k zníženiu rizika zlyhania v počiatočnej fáze,
- odhad času potrebného na odstránenie dôsledkov zlyhania a obnovenie kontinuity činnosti,
- identifikácia alternatív, faktorov, pomocou ktorých je možné zachovať kontinuitu činnosti,
- identifikácia alternatívnych zdrojov, ktoré má organizácia k dispozícii,
- stanovenie nákladov na zachovanie kontinuity činnosti z hľadiska potenciálnej implementácie každého alternatívneho zdroja.

Pridaná hodnota pre organizáciu môže byť dosiahnutá len vtedy, ak sú vykonané odhady a posúdenie rizík podrobné a dôkladné a ich autori sú kompetentní a skúsení v tomto type činnosti¹⁰.

Očakáva sa, že štatutárny orgán alebo ním určené zodpovedné osoby a osoby zodpovedné za riadenie subjektu verejnej správy sa budú podieľať na procesoch posúdenia rizík a bezpečnosti v rôznych oblastiach tým, že:

- určovaním opatrení na riadenie rizík a charakteristík potrebných na ich posudzovanie a kontrolu,
- identifikovaním nositeľov rizík a koordinátora riadenia rizík,
- zabezpečovaním integrácie požiadaviek v každej oblasti bezpečnosti s dozornými kompetenciami pre tieto oblasti a kompetenciami kľúčových zamestnancov poverených vykonávaním najdôležitejších procesov, služieb a špecializovaných úloh súvisiacich s verejným alebo (a) obchodným cieľom,
- zlepšovaním činností a metód posudzovania rizík s cieľom posilniť odolnosť voči hrozbám a podporovať kultúru bezpečnosti,
- zachovaním schopnosti aktualizovať plány riadenia rizík a reakcie na ne v rámci ich cyklického hodnotenia alebo podľa potreby v dôsledku zmien vo vnútornom a vonkajšom bezpečnostnom prostredí,

¹⁰ Strategy on the resilience of critical entities Standards for ensuring the proper operation of critical infrastructure best practices and recommendations. RCB 2025. Dostupné na internete: < <https://www.gov.pl/web/rcb-en/national-critical-infrastructure-protection-program>>.

- „vedením a odhodlaním viesť a podporovať zamestnancov, aby prispievali k účinnosti BCMS¹¹ a jeho propagácii neustáleho zlepšovania, a podporovaním iných relevantných vedúcich úloh s cieľom zdôrazniť ich odhodlanie zahrnuté v ich zodpovednostiach“.

Predkladaná stratégia sa zameriava na zvýšenie odolnosti kritických na SR prostredníctvom implementácie týchto odporúčaní. Kľúčovým predpokladom pre dosiahnutie pridanej hodnoty pre subjekty je ďalšie rozpracovanie prevádzkových rizík. Tieto odporúčania sú nevyhnutné pre vytvorenie cyklického systému posudzovania rizík a bezpečnosti, ktorý prispieva k celkovej odolnosti a stabilite systému na úseku kritickej infraštruktúry.

Zvyšovanie odolnosti je neustály proces, ktorý si vyžaduje plánovanie, investície a neustále prispôsobovanie sa novým hrozbám. Je to o implementácii DRMC – Disaster Risk Management Cycle do všetkých procesov, systémov a podsystémov aby bola správne pochopená prevencia, pripravenosť, adekvátne reakcia a efektívna obnova.

Tak ako cyklus krízového riadenia začína posúdením rizík, aj v oblasti kritickej infraštruktúry je potrebné vykonávať toto posudzovanie nielen na pokyn Ministerstva vnútra SR alebo v súlade s pravidelnými intervalmi určenými právnymi predpismi, ale aj z vlastného rozhodnutia ústredného orgánu, ak to považuje za vhodné alebo ak vyhodnotí, že nastala významná zmena v podmienkach či fungovaní sektora. Rovnako aj v prípadoch, keď sú prijaté zásadné opatrenia na zvýšenie pripravenosti, je vhodné následne vykonať nové posúdenie, aby sa overila účinnosť a vhodnosť prijatých zmien. Takýto prístup umožní včas identifikovať nové riziká, pružne reagovať na vznikajúce hrozby a zabezpečiť, aby boli prijaté opatrenia skutočne efektívne.

¹¹ Systém manažérstva kontinuity podnikania ISO 22301:2019 (BCMS - Business Continuity Management System). ISO 22301 je prijatá do sústavy slovenských technických noriem ako STN EN ISO 22301 Ochrana spoločnosti. Systémy manažérstva kontinuity podnikania. Požiadavky (ISO 22301). Sústavu spravuje Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky ako slovenský národný normalizačný orgán, pričom umožňuje zainteresovaným stranám podieľať sa na ich tvorbe a slovenské technické normy odplatne poskytuje prostredníctvom Portálu noriem.

Záver MV SR

Vzhľadom na svoj rozsah a zložitosť táto správa prináša dôležité príležitosti pre ďalšiu prácu. Prvú časť z nich prináša kapitola v odporúčaných opatreniach na zvýšenie odolnosti kritických subjektov. Druhá časť je prezentovaná v Stratégie odolnosti kritických subjektov.

Vytvorenie, pravidelné preskúmavanie a aktualizácia štandardného zoznamu hrozieb (tab.1) pre sektory kritickej infraštruktúry a pokračovaním dohodnutého procesu identifikácie a definovania hrozieb je základným predpokladom pre rozhodovanie a riadenie založené na riziku. Odporúča sa, aby zoznam hrozieb preskúmali aj kritické subjekty ako koneční používatelia, ktorí zohľadnia vlastné potreby zapojené do znižovania rizika katastrof, riadenia mimoriadnych situácií, zmeny klímy a aktérov usilujúcich sa o udržateľný rozvoj. Je to tiež v súlade s ustanovením Sendajského rámca, podľa ktorého je znižovanie rizika katastrof úlohou celej spoločnosti a všetkých štátnych inštitúcií¹².

Pri skúmaní zoznamu hrozieb je potrebné upozorniť aj na zvyšujúci sa význam a vplyv hybridných hrozieb pôsobiacich súčasne vo viacerých doménach vrátane sektorov kritickej infraštruktúry. Narastajúca nestabilita pochádzajúca z medzinárodnej bezpečnostnej situácie zdôrazňuje potrebu budovania odolnosti. Odolnosť ako schopnosť kritických subjektov vyrovnat' sa s hybridným pôsobením rôznej intenzity spôsobom, ktorý minimalizuje negatívny vplyv a urýchli obnovu funkčnosti zasiahnutých procesov základných služieb je základným predpokladom na zvládanie súčasných i budúcich kríz.

Identifikované zraniteľnosti majú významný potenciál polarizovať spoločnosť, oslabiť celkovú dôveryhodnosť, legitimitu a rozhodovacie procesy štátnych inštitúcií, základných služieb ako aj ohroziť zahraničnopolitické ukotvenie SR.

Hybridné hrozby predstavujú riziká, ktorých vplyv je extrémne ťažké kvantifikovať a hodnotiť. Táto obťažnosť vyplýva z ich podvratnej povahy, synergických účinkov a cielenej nejednoznačnosti. Jednou z najcharakteristickejších vlastností hybridných hrozieb je, že zámerne operujú v „sivej zóne“ s dôrazom za úmyselné vytvorenie podmienok pre pravdepodobné vyhýbanie sa zodpovednosti, s možnosťou popierania zodpovednosti za spáchané incidenty. Hlavným motívom pre tento prístup je získaná asymetrická výhoda. Kombinácia fyzickej hrozby s informačnou manipuláciou môže viesť k panike a nedôvere, čo je omnoho väčší a ťažšie merateľný vplyv, než len technická škoda. Táto dynamika nelineárneho vplyvu je ťažko predvídateľná a ešte ťažšie kvantifikovateľná, pretože závisí od krehkých a dynamických vzťahov medzi jednotlivými základnými službami a ich medzi-sektorových presahov.

Hodnotenie vplyvu hybridných hrozieb je inherentne ťažké kvôli ich nejednoznačnej a synergickej povahe. Kvantifikácia si vyžaduje ďalšie analytické nástroje a modely. Dôsledky na dôveru obyvateľstva sú ambivalentné a nepredvídateľné. Dezinformácie erodujú dôveru v tradičné piliere spoločnosti, zatiaľ čo môžu paradoxne posilňovať dôveru v iné segmenty.

Fyzická a kybernetická odolnosť sektorov kritickej infraštruktúry je kľúčovou obranou proti hybridným útokom. Keď infraštruktúra úspešne odolá cielenému útoku a služby zostanú funkčné, je to dôkaz funkčnosti systému a posilní to pocit stability. Zabezpečenie fyzickej odolnosti prostredníctvom regulácie zákona č. 367/2024 Z. z. o kritickej infraštruktúre paralelne

¹²Hazard definition & classification review technical report. 2020 UNITED NATIONS. Dostupné na internete: <<https://www.undrr.org/media/47681/download?startDownload=20251110>>.

s zákonom č. 69/2018 Z. Z. o kybernetickej bezpečnosti zabezpečia integrovaný prístup aj voči rizikám, ktoré hybridné hrozby predstavujú.