STRATÉGIA ODOLNOSTI KRITICKÝCH SUBJEKTOV SR

ZOZNAM POUŽITÝCH SKRATIEK

EK	Európska komisia
EÚ	Európska únia
CERG	Skupina pre odolnosť kritických subjektov
DG ECHO	Generálne riaditeľstvo civilnej ochrany a humanitárnej pomoci
DG HOME	Generálne riaditeľstvo pre migráciu a vnútorné záležitosti
JISKB	Jednotný informačný systém kybernetickej bezpečnosti
MD SR	Ministerstvo dopravy Slovenskej republiky
MF SR	Ministerstvo financií Slovenskej republiky
MH SR	Ministerstvo hospodárstva Slovenskej republiky
MIRRI SR	Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky
MO SR	Ministerstvo obrany Slovenskej republiky
MPRV SR	Ministerstvo pôdohospodárstva a rozvoja vidieka Slovenskej republiky
MV SR	Ministerstvo vnútra Slovenskej republiky
MZ SR	Ministerstvo zdravotníctva Slovenskej republiky
MŽP SR	Ministerstvo životného prostredia Slovenskej republiky
NATO	Organizácia Severoatlantickej zmluvy
NBAC	Národné bezpečnostné analytické centrum
NBS	Národná banka Slovenska
NBÚ	Národný bezpečnostný úrad
PROCIV	Pracovná skupina pre civilnú ochranu
SAV	Slovenská akadémia vied
SR	Slovenská republika
UCPM	Mechanizmus Únie v oblasti civilnej ochrany
ÚOŠS SR	Ústredné organy štátnej správy Slovenskej republiky
ÚV SR	Úrad vlády Slovenskej republiky

OBSAH

1. ÚVOD A VÝCHODISKÁ DOKUMENTU

Bezpečnostné prostredie je dnes charakteristické vysokou mierou dynamickosti, prepojenosti a závislostí. Hrozby už nie sú izolované, ale majú tendenciu vytvárať reťazové efekty. Nešíria sa len naprieč sektormi kritickej infraštruktúry, ale ovplyvňujú mnohé ďalšie oblasti, na ktorých je dnes moderná spoločnosť a demokratický systém postavený. To, čo začne ako incident týkajúci sa jedného kritického subjektu, môže rýchlo ovplyvniť ďalšiu bezpečnostnú alebo hospodársku oblasť, pri najzávažnejších incidentoch dokonca celý systém.

Podľa článku 2 smernice Európskeho parlamentu a Rady (EÚ) 2022/2557 zo 14. decembra 2022 o odolnosti kritických subjektov a o zrušení smernice Rady 2008/114/ES (ďalej len „smernica CER"), je odolnosť definovaná ako „schopnosť subjektu predchádzať narušeniam, odolávať im, prispôsobiť sa im a spamätať sa z nich". Takto vymedzený pojem odolnosť by sa mal chápať aj ako schopnosť kritického subjektu predchádzať udalostiam, ktoré výrazne narúšajú alebo môžu významne narušiť poskytovanie základných služieb v rámci vnútorného trhu, t. j. služieb, ktoré sú kľúčové pre zachovanie nevyhnutných spoločenských a hospodárskych funkcií, verejnej bezpečnosti a ochrany zdravia obyvateľstva alebo životného prostredia, chrániť pred takýmito udalosťami, reagovať na ne, odolávať im, zmierňovať ich, absorbovať ich, prispôsobovať sa im alebo zotaviť sa z nich.

Zhoršené bezpečnostné prostredie vyžaduje budovanie odolnosti, a naopak, silná odolnosť priamo formuje a posilňuje bezpečnostné prostredie štátu a celej spoločnosti. Vzťah medzi odolnosťou a bezpečnostným prostredím je teda obojsmerný. Z európskej perspektívy bezpečnostné prostredie zmenili najviac udalosti ako migrácia, pandémia COVID-19 a vojnový konflikt na Ukrajine. Vplyvom udalostí sa do popredia dostali aj nové bezpečnostné fenomény, ako sú kybernetické, informačné a hybridné hrozby. Okrem toho existuje zvýšené fyzické riziko v dôsledku prírodných katastrof a zmeny klímy, ktorá zintenzívňuje frekvenciu a rozsah extrémnych výkyvov počasia a prináša dlhodobé zmeny priemerných klimatických podmienok, ktoré môžu znížiť kapacitu, efektívnosť a životnosť určitých typov infraštruktúry, ak sa nezavedú opatrenia na adaptáciu na zmenu klímy.

Ostatné správy o bezpečnosti SR hodnotia celkovú bezpečnostnú situáciu v SR ako stabilnú. Bezpečnostné prostredie SR vnímajú cez vojnový konflikt na Ukrajine, kde pravdepodobnosť rozšírenia vojny označuje za minimálnu, no riziko neúmyselného zasiahnutia územia SR v dôsledku pokračujúcich bojov stále nemožno vylúčiť[1]. Medzi najväčšie bezpečnostné hrozby, ktoré dlhodobo ovplyvňujú bezpečnostné prostredie v Európe, patrí terorizmus. V súčasnosti platí na území SR zvýšený 2. stupeň teroristického ohrozenia 4-stupňovej škály), ktorý reflektuje na pretrvávajúce teroristické hrozby v niektorých európskych štátoch, ako aj na bezpečnostnú situáciu v SR. Toto tvrdenie podporuje aj Hodnotenie hrozieb závažnej a organizovanej trestnej činnosti v EÚ za rok 2025[2].

[1] Správa o bezpečnosti Slovenskej republiky - nové znenie. 2023. Dostupné na internete: <https://rokovania.gov.sk/RVL/Material/31003/1>.

[2] Stratégia EÚ na boj proti organizovanej trestnej činnosti na roky 2021 – 2025 (Európska komisia). Dostupné na internete: < https://www.consilium.europa.eu/sk/policies/eu-fight-against-crime/>.

Správa o bezpečnosti SR je jediný verejný dokument, ktorý hodnotí ochranu kritickej infraštruktúry SR, avšak cez pohľad energetickej bezpečnosti. Predpokladom kontinuity základných služieb všetkých ostatných sektorov kritickej infraštruktúry je sektorová závislosť na energetike. Preto sa na túto infraštruktúru vzťahuje prezumpcia tzv. „overriding public interest" – prevažujúci verejný záujem[3]. Správa o bezpečnosti SR primerane zachytáva vojensko-bezpečnostný rozmer hodnoteného obdobia, avšak nereflektuje vyčerpávajúco rizikový profil kritickej infraštruktúry v podmienkach súčasného nestabilného geopolitického prostredia a dynamického vývoja umelej inteligencie, ktorá sa čoraz viac využíva ako nástroj kybernetických a hybridných hrozieb, zvyšuje sofistikovanosť útokov a komplikuje včasnú identifikáciu rizík. Vzhľadom na aktuálne medzinárodné hodnotenia bezpečnosti[4] sú za kľúčovú a rastúcu hrozbu pre kritickú infraštruktúru považované kybernetické bezpečnostné incidenty. Kritická infraštruktúra je v tomto kontexte vnímaná ako primárny objekt záujmu, vystavený kombinovanému tlaku kybernetických, kriminálnych, teroristických a environmentálnych hrozieb, ktoré sa v podmienkach prehlbujúcej sa geopolitickej konfrontácie navzájom posilňujú. Potenciálne následky a škody spôsobené narušením kritickej infraštruktúry sú zároveň z pohľadu útočníkov mimoriadne atraktívne, keďže umožňujú dosiahnuť vysoký bezpečnostný, ekonomický aj spoločenský vplyv. Medzinárodné správy zároveň poukazujú na to, že pokročilé pretrvávajúce hrozby (angl. Advanced Persistent Threaths - APT) sa dlhodobo „predumiestňujú" v sieťach kritických subjektov s cieľom pripraviť podmienky na budúce kybernetické útoky, ktoré môžu byť aktivované vo vhodnej, útočníkom zvolenej chvíli. Rozvoj kvantových technológií zásadne mení prostredie kybernetickej bezpečnosti[5]. Kybernetické útoky na subjekty kritickej infraštruktúry patria medzi najzávažnejšie bezpečnostné hrozby, vykazujú rastúci trend a sú realizované tak štátom podporovanými aktérmi v rámci hybridných operácií, ako aj organizovanými kriminálnymi sieťami motivovanými finančným ziskom, pričom dostupnosť útočných nástrojov a služieb v prostredí „zločinu ako služby" podstatne znižuje nároky na ich realizáciu. Z európskej perspektívy je rozsah hrozieb široký[6]. Ako ďalej popisuje európska stratégia vnútornej bezpečnosti, hybridné hrozby narúšajú demokratické procesy, snažia sa zasahovať aj do dodávateľských reťazcov a narušiť ich, hľadajú spôsoby ako kradnúť citlivé údaje a využiť ich pre svoje pozície, čo má za následok ohrozenie fungovania základných služieb, ktoré kritické subjekty poskytujú.

2. Zámer a strategické ciele

Odolnosť je základným predpokladom na zvládanie moderných bezpečnostných výziev vo všeobecnosti. Uvedené platí aj na úseku kritickej infraštruktúry. Samotná odolnosť pritom nie je

[3] Z tohto dôvodu sa v európskej energetickej legislatíve (RePowerEU, RED III, TEN-E, Net Zero Industry Act) ako aj v národnej (transpozícia RED III) zavádza princíp, podľa ktorého sa energetická infraštruktúra, považuje za súčasť prevažujúceho verejného záujmu.

[4] Global Risks Report .2025. World Economic Forum. Dostupné na internete: <https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf>. European Union Terrorism Situation and Trend report. 2025. (EU TE-SAT) Dostupné na internete: < https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2025-eu-te-sat>.

[5] Rozvoj kvantových technológií podrobnejšie zohľadňuje Národná stratégia kybernetickej bezpečnosti na roky 2026 až 2030.

[6] ProtectEU: európska stratégia vnútornej bezpečnosti. 2025. Stratégia EÚ na boj proti organizovanej trestnej činnosti na roky 2021 – 2025 (Európska komisia). Dostupné na internete: < https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52025DC0148>.

len o prevencii, ale aj o pripravenosti na potenciálnu hrozbu a jej preniknutie. Nedostatočná odolnosť a nezvládnuté reťazové efekty majú hlboké a rozsiahle následky, ktoré ďaleko presahujú hospodárske škody, sociálne a bezpečnostné dopady.

Vývoj koncepcií kritickej infraštruktúry v SR musí preto prejsť od pasívneho prístupu k aktívnemu. V pôvodnom modeli ochrany a obrany prvkov kritickej infraštruktúry absentovali dynamické opatrenia a zameriaval sa skôr na statické a reaktívne opatrenia po vzniku udalosti. Naopak, ostatné legislatívne zmeny v oblasti kritickej infraštruktúry majú za cieľ nahradiť tento prekonaný model robustnejším, proaktívnym systémom. Tento systém sa zakladá na troch kľúčových cieľoch:

Cieľ č. 1: Proaktívny prístup: Potreba prechodu od reaktívneho k proaktívnemu prístupu**:** Reagovanie na hrozby sa nahradí dôrazom na systematické predvídanie, monitorovanie a plánovanie. Nové opatrenia sa snažia identifikovať potenciálne riziká skôr, než sa naplnia.

Cieľ č. 2: Posilnenie plánovania a reakcie: Vytvorenie dynamického systému s jasnými postupmi pre rôzne typy hrozieb. To zahŕňa aj lepšiu koordináciu medzi štátnymi orgánmi a kritickými subjektami.

Cieľ č. 3: Komplexný prístup k odolnosti: Zmena filozofie ochrany kritickej infraštruktúry, ktorá sa neobmedzuje len na fyzickú bezpečnosť, ale zahŕňa aj schopnosť rýchlo sa zotaviť z narušení spôsobených kybernetickými bezpečnostnými incidentmi, prírodnými katastrofami, ľudskými, dodávateľskými alebo organizačnými systémovými zlyhaniami, inými technogénnymi a asymetrickými hrozbami.

Cieľom Stratégie odolnosti kritických subjektov (ďalej len „stratégia“) podľa § 7 zákona č. 367/2024 Z. z. o kritickej infraštruktúre a o zmene a doplnení niektorých zákonov (ďalej len „zákon o kritickej infraštruktúre“) a s odkazom na smernicu CER, je definovať opatrenia na zvýšenie odolnosti kritickej infraštruktúry, a to nielen pokiaľ ide o pripravenosť, ale aj o koordinovanú reakciu. Obsahom stratégie sú jednotlivé úlohy, ktoré umožnia dosiahnuť čo najefektívnejší prístup k budovaniu odolnosti kritických subjektov v SR.

3. BUDOVANIE ODOLNOSTI NA ÚSEKU KRITICKEJ INFRAŠTRUKTÚRY

CIEĽ Č. 1: PROAKTÍVNY PRÍSTUP

Posun od reaktívneho k proaktívnemu prístupu poukazuje na rastúce povedomie, že ochrana kritickej infraštruktúry je v dnešnom globálne prepojenom svete kľúčová pre zabezpečenie základných služieb pre obyvateľstvo a pre ďalšie fungovanie trhu. Nové opatrenia preto majú za cieľ vytvoriť komplexnejší a odolnejší systém schopný lepšie čeliť moderným hrozbám.

Cesta k cieľovému stavu

Prvým krokom je identifikácia hrozieb a posúdenie rizík. Bez hlbokého pochopenia potenciálnych hrozieb a ich pravdepodobného vplyvu, nie je možné efektívne alokovať zdroje a vypracovať vhodné protiopatrenia. Nová legislatíva v podobe zákona o kritickej infraštruktúre vyžaduje pravidelné hodnotenie rizík kritickými subjektmi. Zámerom je pochopiť najväčšie hrozby a zmierniť ich riziko, ako aj dôsledky (v prípade preniknutia). Pri posudzovaní rizík[7], vyplývajúcich z bezpečnostného prostredia na úseku kritickej infraštruktúry, vplývajú na poskytovanie základnej služby bezpečnostné hrozby, ako sú kybernetické útoky, zraniteľnosť dodávateľského reťazca a hybridné hrozby. Identifikovať a posudzovať riziká na úseku kritickej infraštruktúry podľa § 8 zákona o kritickej infraštruktúre si dáva za úlohu aj táto stratégia. V prílohe č. I stratégia odkazuje na dokument Posúdenie rizík v sektoroch kritickej infraštruktúry SR, ktorý popisuje postup identifikácie hrozieb a posúdenie rizík v sektoroch kritickej infraštruktúry v SR. Tento dokument slúži ako nástroj na zabezpečenie znalostí o existujúcich hrozbách a potenciálnych zraniteľnostiach.

Na zabezpečenie odolnosti je nevyhnutné mať prehľad a znalosti o všetkých relevantných hrozbách, ktorým sú kritické subjekty vystavené. Na tento účel sa podľa § 8 zákona o kritickej infraštruktúre vykoná posúdenie rizík vždy, keď je to potrebné vzhľadom na osobitnú situáciu a vývoj predmetných rizík, najmenej však každé štyri roky.

Posúdenie rizík, ktoré vykonávajú kritické subjekty, bude vychádzať z posúdenia rizika, ktoré vykonali ústredné orgány na úseku kritickej infraštruktúry[8] a sprístupnili im ho. Rešpektujúc zákon o kritickej infraštruktúre, podsektory Jadrová energetika, Digitálna infraštruktúra a Financie sú z popisu tejto úlohy vyňaté z dôvodu povinností upravených podľa osobitných predpisov[9].

---

[7] pozri prílohu č. I Posúdenie rizík v sektoroch kritickej infraštruktúry SR

[8] Odolnosť kritickej infraštruktúry je v SR prierezová agenda v pôsobnosti viacerých ústredných orgánov štátnej správy podľa § 3 písm. c) zákona o kritickej infraštruktúre.

[9] Subjekty v sektore Energetika, podsektore Jadrová energetika, ktoré začnú poskytovať základné služby podľa zákona o kritickej infraštruktúre sa riadia podľa § 20 zákona o kritickej infraštruktúre. Orgán štátnej správy vykonáva reguláciu a dohľad podľa § 4 zákona č. 541/2004 Z. z. o mierovom využívaní jadrovej energie (atómový zákon) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. Subjekty v sektore Financie, podsektore Bankovníctvo a Finančné trhy plnia povinnosti podľa osobitných predpisov v oblasti finančného trhu, najmä zákon č. 483/2001 Z. z. o bankách a o zmene a doplnení niektorých zákonov a nariadenie DORA. Subjekty v sektore Financie, podsektore Systémy riadenia verejných financií a v sektore Digitálna infraštruktúra plnia povinnosti podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov“. Kritické subjekty plnia povinnosti v oblasti informačných technológií verejnej správy podľa zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a vykonávacích predpisov (vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy v znení neskorších predpisov, vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných

Úloha	Popis úlohy	Zodpovedný subjekt	Súčinný subjekt	Časový horizont realizácie
č. 1	Sprístupniť relevantné časti posúdenia rizika v príslušnom sektore a podsektore podľa prílohy č. 1 podľa zákona o kritickej infraštruktúre kritickým subjektom na účely vykonania posúdenia rizík kritickým subjektom.	MV SR, MH SR, MD SR, MIRRI SR, SŠHR SR, MŽP SR, MPRV SR	Všetky kritické subjekty okrem výnimiek podľa § 19 ods. 3 zákona o kritickej infraštruktúre.	najneskôr do 17. júla 2026.

Budovanie odolnosti si vyžaduje objektívne posúdenie vlastných zraniteľností a nedostatkov. Je nevyhnutné uvažovať a premýšľať v intenciách najhorších scenárov, ktoré sú základným pilierom pripravenosti na krízové situácie. Zvýšenie pripravenosti a pohotovosti na novú úroveň zároveň prispeje k zníženiu rozsahu a závažnosti faktorov, ktoré by mohli viesť k incidentom a krízam. Správne, účinne a trvalo udržateľne vykonaná príprava na celý rozsah možných rizík posilní budovanie odolnosti, čím sa docieli silný preventívny účinok. Z toho dôvodu sa navrhuje v úlohe č. 2 posilniť rozvoj aktívnej odbornej spolupráce, napr. s akademickou obcou alebo inými vedeckými inštitúciami, s cieľom zlepšovať implementáciu osvedčených postupov a medzinárodných štandardov a pomáhať postupne rozvíjať koherentnú a konzistentnú metodiku hodnotenia rizík a hrozieb podľa navrhovanej metodiky v prílohe č. I.

Úloha	Popis úlohy	Zodpovedný subjekt	Súčinný subjekt	Časový horizont realizácie
č. 2	Zabezpečiť vhodný nástroj na efektívne vzdelávanie v oblasti posudzovania rizík v sektoroch kritickej infraštruktúry pre pracovníkov kritických subjektov a štátnych zamestnancov s agendou kritickej infraštruktúry, krízového riadenia a bezpečnosti k posudzovaniu rizík podľa osobitných predpisov[10].	MH SR, MIRRI SR, SŠHR SR, NBÚ, MF SR, MŽP SR, MPRV SR, MV SR	Spolupráca s akademickou obcou a výskumnými inštitúciami.	Najneskôr do 31. januára 2027.

technológií verejnej správy, vyhláška Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. 401/2023 Z. z. o riadení projektov a zmenových požiadaviek v prevádzke informačných technológií verejnej správy v znení vyhlášky č. 46/2025 Z. z.)

[10] Napríklad nariadenie Európskeho parlamentu a Rady (EÚ) 2017/1938 z 25. októbra 2017 o opatreniach na zaistenie bezpečnosti dodávok plynu a o zrušení nariadenia (EÚ) č. 994/2010 (Ú. v. EÚ L 280, 28. 10. 2017) v platnom znení, nariadenie Európskeho parlamentu a Rady (EÚ) 2019/941 z 5. júna 2019 o pripravenosti na riziká v sektore elektrickej energie a o zrušení smernice 2005/89/ES

Hlavným výstupom bude doplnená metodika a systém posúdenia východiskových sektorových rizík v prílohe č. I, čo v konečnom dôsledku podporí metodiku a proces interného posúdenia rizík na úrovni jednotlivých kritických subjektov, čím sa dokončí životný cyklus analýzy rizík na úseku kritickej infraštruktúry. Ďalšie sektorové metodiky musia nadväzovať na už existujúcu všeobecnú metodiku analýzy rizík pre uplatnenie v procesoch riadenia rizika aj v zmysle požiadaviek podľa osobitných predpisov[11].

Pretože prevádzkovanie základných služieb čelí širokému spektru hrozieb, je dôležité, aby ústredné orgány na úseku kritickej infraštruktúry aj kritické subjekty disponovali plánmi reakcie, kontinuity[12] činností a obnovy, ktoré umožnia udržať základné služby počas kríz. Pravidelná aktualizácia týchto plánov minimalizuje riziko ich nefunkčnosti, skracuje čas prerušenia služieb a posilňuje dôveru verejnosti v ich spoľahlivosť.

CIEĽ Č. 2: POSILNENIE PLÁNOVANIA A REAKCIE

Zámerom tohto cieľa je lepšia koordinácia a výmena informácií. Nové opatrenia musia podporiť efektívnejšiu komunikáciu medzi ústrednými orgánmi navzájom, ako aj medzi ústrednými orgánmi a kritickými subjektami. To pri včasnom varovaní a koordinovanej reakcii pomôže opatreniam týkajúcim sa obnovy služieb a v konečnom dôsledku získaným znalostiam o hrozbách.

Cesta k cieľovému stavu

Vytvorenie komunikačných kanálov na nahlasovanie bezpečnostných incidentov podporuje proaktívny a koordinovaný prístup k celkovej odolnosti. Hlavným zámerom je zabezpečenie mechanizmu oznamovania incidentov, ktorý by umožnil rýchlo a primerane reagovať na incidenty a získať komplexný prehľad o vplyve, povahe, príčinách a možných dôsledkoch incidentov, ktoré kritické subjekty riešia. Kritické subjekty musia bez zbytočného odkladu informovať príslušné orgány o incidentoch, ktoré významne narúšajú alebo majú potenciál významne narušiť poskytovanie základných služieb. Neustály zber a analýza informácií o hrozbách, na základe ktorých by ústredné orgány vydávali, zasielali a vyhlasovali včasné varovania, výstrahy a odporúčania pre kritické subjekty, zabezpečuje úloha č. 3. Vzájomná interoperabilita s JISKB musí byť zabezpečená s ohľadom na § 14 ods. 9 zákona o kritickej infraštruktúre.

(Ú. v. EÚ L 158, 14. 6. 2019), zákon č. 747/2004 Z. z., zákon č. 7/2010 Z. z. o ochrane pred povodňami v znení neskorších predpisov, zákon č. 128/2015 Z. z. o prevencii závažných priemyselných havárií a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, § 8 zákona o kritickej infraštruktúre.

[11] Napríklad nariadenie Európskeho parlamentu a Rady (EÚ) 2017/1938 z 25. októbra 2017 o opatreniach na zaistenie bezpečnosti dodávok plynu a o zrušení nariadenia (EÚ) č. 994/2010 (Ú. v. EÚ L 280, 28. 10. 2017) v platnom znení, nariadenie Európskeho parlamentu a Rady (EÚ) 2019/941 z 5. júna 2019 o pripravenosti na riziká v sektore elektrickej energie a o zrušení smernice 2005/89/ES (Ú. v. EÚ L 158, 14. 6. 2019), zákon č. 747/2004 Z. z., zákon č. 7/2010 Z. z. o ochrane pred povodňami v znení neskorších predpisov, zákon č. 128/2015 Z. z. o prevencii závažných priemyselných havárií a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, § 8 zákona o kritickej infraštruktúre.

[12] Plány kontinuity sa vypracúvajú podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a vyhlášky Národného bezpečnostného úradu č. 227/2025 Z. z. o bezpečnostných opatreniach.

Úloha	Popis úlohy	Zodpovedný subjekt	Súčinný subjekt	Časový horizont realizácie
č. 3	Zabezpečiť vhodný spôsob nahlasovanie incidentov[13] a zdieľanie informácií[14] o kritickej infraštruktúre podľa § 14 ods. 1 a 2, 4 až 9 zákona o kritickej infraštruktúre.	MV SR	MH SR, MD SR, MIRRI SR, SŠHR SR, MZ SR, NBÚ, MF SR, MŽP SR, MPRV SR, SIS, MO SR	December 2027

Riešenie na nahlasovanie incidentov a zdieľanie informácií o kritickej infraštruktúre má zabezpečiť rýchly a efektívny zber, spracovanie a distribúciu informácií o bezpečnostných incidentoch a neočakávaných udalostiach. Riešenie na nahlasovanie incidentov v kritickej infraštruktúre musí byť navrhnuté s ohľadom na vysokú dostupnosť, dôvernosť a integritu dát a bude súčasťou pripravovanej integrácie a modernizácie informačných systémov MV SR. Vzájomná integrácia a interoperabilita s ostatnými informačnými systémami ako súčasť väčšieho celku si kladie za cieľ vytvoriť jednotné dátové prostredie jednotlivých zložiek a útvarov MV SR. Tento projekt je plánovaný ako súčasť širšej modernizácie systémov MV SR a využíva synergie tejto modernizácie.

Kritické subjekty sú povinné v prípade incidentu predložiť prvé oznámenie najneskôr do 24 hodín po tom, ako nadobudli o incidente vedomosť. Prvotné oznámenie obsahuje informácie, ktoré sú nevyhnutne potrebné na to, aby príslušné orgány nadobudli o incidente vedomosť a v prípade potreby umožnili kritickému subjektu požiadať o pomoc. Ak je to možné, v takomto oznámení sa uvedie predpokladaná príčina incidentu. Po prvotnom oznámení sa v prípade potreby zasiela podrobná správa najneskôr do jedného mesiaca po incidente. Podrobná správa dopĺňa pôvodné oznámenie a poskytuje komplexný prehľad o incidente.

Vzhľadom na rastúcu digitalizáciu procesov a služieb, ako aj na kumuláciu vojenských, geopolitických, technologických a environmentálnych hrozieb, ktorým kritická infraštruktúra čelí, sú aktuálne legislatívne zmeny osobitne zamerané na posilnenie kybernetickej bezpečnosti ako kľúčového prvku jej odolnosti. Kybernetická bezpečnosť v tomto kontexte predstavuje vysoko prierezovú oblasť zasahujúcu všetky sektory kritickej infraštruktúry a jej posilňovanie v podobe spoločného strategického piliera má zabezpečiť synergie medzi sektormi a jednotný rámec prevencie, monitorovania a reakcie na hrozby.

Kritické subjekty sú povinné venovať osobitnú pozornosť kybernetickej odolnosti ako je ochrana informačných a komunikačných systémov[15], riadeniu rizík v dodávateľských reťazcoch, zabezpečeniu kontinuity prevádzky a riadenému zvládaniu kybernetických bezpečnostných incidentov, ako aj systematickému zvyšovaniu povedomia a odbornej pripravenosti zamestnancov, ktorí predstavujú jeden z najzraniteľnejších prvkov celkového bezpečnostného systému.

[13] Hlásenie kybernetických bezpečnostných incidentov, rozsahu oznamovaných údajov a harmonogramu podávania situačných hlásení v období kybernetickej krízy je upravené osobitnými právnymi predpismi (najmä zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a vyhláškou Národného bezpečnostného úradu č. 226/2025 Z. z., ktorou sa ustanovujú podrobnosti o hláseniach).
[14] Podľa zákona č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov.
[15] Podľa zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov.

Systematické a jednotné začlenenie kybernetickej bezpečnosti do strategických, riadiacich a plánovacích procesov kritických subjektov, v spojení s dôslednou implementáciou príslušnej legislatívy, predstavuje nevyhnutný predpoklad na zvyšovanie odolnosti kritickej infraštruktúry, celkovej bezpečnosti štátu a ochranu verejných záujmov.

Je kľúčové, aby subjekty venovali osobitnú pozornosť zabezpečeniu a kontinuite prevádzky a reagovaniu na incidenty, pretože ich odolnosť má priamy vplyv na celkovú bezpečnosť štátu. Systematické a jednotné začlenenie kybernetickej bezpečnosti do stratégie je nevyhnutným predpokladom pre dosiahnutie cieľa, ktorým je zvyšovanie odolnosti kritických subjektov a ochrana verejných záujmov.

Podľa § 12 zákona o kritickej infraštruktúre pre komunikáciu a nahlasovanie incidentov na úseku kritickej infraštruktúry je potrebné viesť verifikáciu kontaktných osôb a spravovať ich zoznam. MV SR ako administrátor informačného systému bude povoľovať vstup do informačného systému a spravovať kontá a prístupy úrovne rolí na základe podkladov od ústredných orgánov na úseku kritickej infraštruktúry. Ústredný orgán na úseku kritickej infraštruktúry vedie zoznam všetkých incidentov, ktoré ovplyvnili poskytovanie základných služieb a informuje o nich MV SR. Následne MV SR informuje ďalšie relevantné bezpečnostné zložky a medzinárodných partnerov[16]. V rámci zabezpečenia plnej implementácie úlohy č. 3 je potrebné nadviazať úlohami č. 4 a č. 5 na zabezpečenie plynulej komunikácie a koordinácie medzi kritickými subjektmi a ústrednými orgánmi z rôznych sektorov, aby sa zabránilo reťazovým dopadom.

Úloha	Popis úlohy	Zodpovedný subjekt	Súčinný subjekt	Časový horizont realizácie
č. 4	Vytvoriť informačnú maticu kontaktných osôb podľa § 12 zákona o kritickej infraštruktúre pre komunikáciu a nahlasovanie incidentov na úseku kritickej infraštruktúry.	MV SR, MH SR, MD SR, MIRRI SR, SŠHR SR, NBÚ, MF SR, MŽP SR, MPRV SR, MZ SR	MO SR, SIS	Od júla 2026 a priebežne podľa potreby.
č. 5	Implementovať informačnú maticu kontaktných osôb do informačného systému na nahlasovanie incidentov kritickej infraštruktúre a jej test.	MV SR, NBÚ	MH SR, MD SR, MIRRI SR, SŠHR SR, NBÚ, MF SR, MŽP SR, MZ SR, MPRV SR, MO SR, SIS,	Marec 2027

Test realizovaného riešenia sa navrhuje na úrovni „table top exercise“, kde súčinné kritické subjekty na základe scenárov z posúdenia rizík v sektoroch kritickej infraštruktúry SR simulujú incident a zasielajú o ňom hlásenie. Následne sa preverí distribúcia správ cez stanovené komunikačné kanály vo všetkých prístupoch a na všetkých úrovniach vrátane interoperability s JISKB.

[16] podľa § 14 ods. 9 zákona o kritickej infraštruktúre.

Kompetencie koordinácie bezpečnostných politík a riadenia bezpečnostných hrozieb na úseku kritickej infraštruktúry možno definovať ako vnútroštátny mechanizmus organizovaný a fungujúci prostredníctvom koordinovaného a aktívneho procesu. Musí zahŕňať analýzu situácie, formuláciu politík, opatrení a implementáciu, monitorovanie a pravidelné preskúmavanie činností, zameraných na znižovanie rizík bezpečnostných hrozieb[17] na úseku kritickej infraštruktúry.

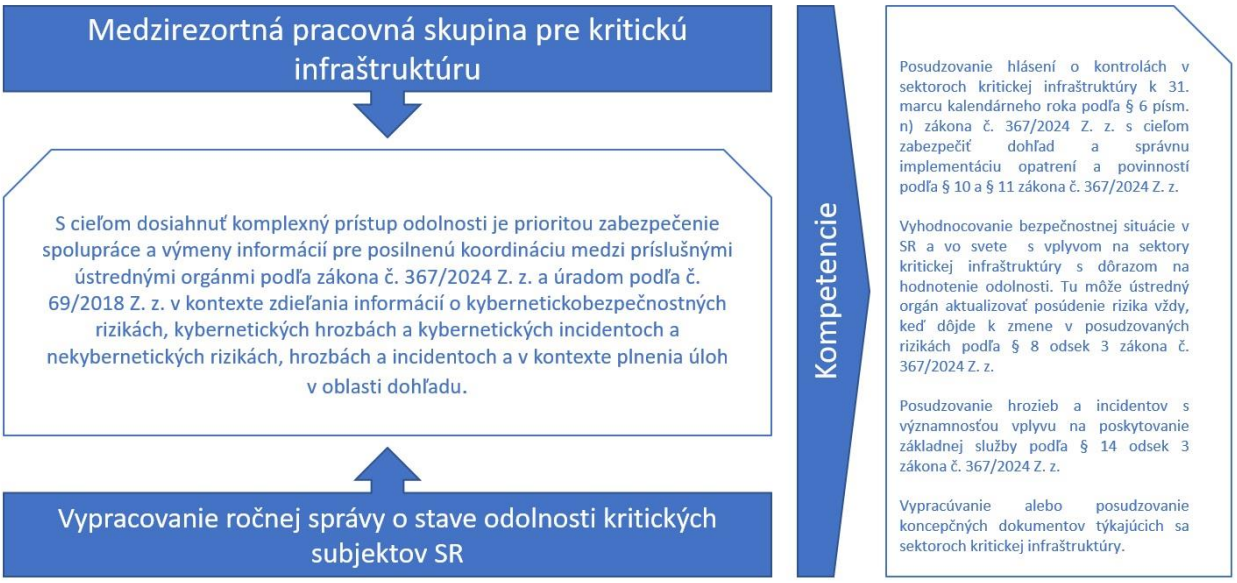
V spomínaných súvislostiach sa odporúča zriadenie **stálej medzirezortnej skupiny pre kritickú infraštruktúru na základe uznesenia vlády SR** (ďalej len „skupina“)**.** Skupina[18] bude odborným prvkom pre rámec na koordináciu medzi orgánmi štátnej správy na úseku kritickej infraštruktúry a na úseku kybernetickej bezpečnosti ako koordinačná, metodická a konzultatívna skupina pre zabezpečenie kontinuity prvkov bezpečnostného systému. V rámci svojich kompetencií koordinuje, usmerňuje, monitoruje, a vyhodnocuje plnenie úloh jednotlivých orgánov, ktoré na základe všeobecne záväzných právnych predpisov riadia procesy zaisťovania kontinuity poskytovania základných služieb. Cieľom skupiny, ktorá bude zložená z nominovaných expertov ústredných orgánov na úseku kritickej infraštruktúry, bude koordinácia a uľahčenie medzirezortnej spolupráce, poskytovanie expertnej bázy pre systematické riešenia a angažovanosť v prioritných činnostiach na úseku kritickej infraštruktúry, ako aj koordinácia reakcií na incidenty a hrozby. Skupina tiež bude poskytovať konzultácie a odborné poradenstvo kritickým subjektom v rámci úlohy č. 4.

Úloha	Popis úlohy	Zodpovedný subjekt	Súčinný subjekt	Časový horizont realizácie
č. 6	Zriadiť stálu medzirezortnú skupinu pre kritickú infraštruktúru na základe uznesenia vlády SR.	MV SR	MH SR, MD SR, MIRRI SR, SŠHR SR, NBÚ, MF SR, NBS, MŽP SR, MZ SR, MPRV SR, MO SR, SIS, ÚV SR	Do 31. marca 2026
č. 7	Pripraviť ročnú správu o vyhodnotení bezpečnostnej situácie na úseku kritickej infraštruktúry.	MV SR	MH SR, MD SR, MIRRI SR, SŠHR SR, NBÚ, MF SR, MŽP SR, MZ SR, MPRV SR, MO SR, SIS	Každoročne do 30. júna.

Skupina[19] bude zodpovedná za koordináciu, plánovanie a implementáciu opatrení na zabezpečenie odolnosti kritických subjektov. V zmysle úlohy č. 7 sa v rámci skupiny pripraví ročná

[17] Dôraz bol v tejto súvislosti orientovaný na splnenie uznesenia vlády č. 65 z 26. januára 2022 k Národnej stratégii riadenia rizík bezpečnostných hrozieb Slovenskej republiky.
[18] Členovia podľa § 3 písm. c) zákona o kritickej infraštruktúre vrátane MO SR, SIS. Podľa vecného programu budú prizývaní ad hoc zástupcovia ostatných štátnych orgánov.
[19] Kontext: EÚ prijala opatrenia na posilnenie odolnosti kritickej infraštruktúry. Smernica (EÚ) 2022/25571 o odolnosti kritických subjektov (smernica CER) bola transponovaná do národnej legislatívy SR v podobe zákona o kritickej infraštruktúre s účinnosťou od 1.1.2025. Smernicou CER a revidovanou smernicou (EÚ) 2022/25552 (smernica NIS2) sme vstúpili do novej fázy spolupráce na

správa o vyhodnotení bezpečnostnej situácie na úseku kritickej infraštruktúry navrhuje predkladať každoročne do 30. júna. Správa bude vychádzať okrem iného aj z aktuálneho posúdenia rizík, z hlásení o kontrole v kritických subjektoch (úloha č. 9) a z hlásení o incidentoch podľa § 14 zákona o kritickej infraštruktúre.



CIEĽ Č. 3: KOMPLEXNÝ PRÍSTUP K ODOLNOSTI

Odolnosť si vyžaduje aj podporné opatrenia a príležitosti na rozvíjanie schopností. Stratégia si v rámci ďalšieho budovania schopností dáva nasledujúce úlohy, ktoré posilnia celkový prístup zvyšovania odolnosti.

Aplikáciou ďalších úloh do praxe sa dosiahne rámec zmien potrebných v bezpečnostnom prostredí, ktoré umožnia zabezpečiť nepretržitú spôsobilosť na úseku kritickej infraštruktúry a poskytovať kontinuálne základné služby podľa prílohy č. 1 zákona o kritickej infraštruktúre.

úrovni EÚ. Tieto dve smernice spoločne vytvárajú rámec na ochranu kritickej infraštruktúry pred kybernetickými aj nekybernetickými hrozbami. Smernica CER má za cieľ posilniť nekybernetickú odolnosť kritických subjektov, ktoré poskytujú „životne dôležité“ základné služby v 11 sektoroch. Prechádza od obmedzenejšieho konceptu ochrany kritickej infraštruktúry k komplexnejšiemu konceptu odolnosti kritických subjektov, pričom sa zameriava na nepretržitú funkčnosť a poskytovanie služieb pred, počas a po narušujúcich incidentoch. Kritické subjekty budú musieť vykonávať posúdenia rizík, prijímať opatrenia na posilnenie odolnosti a oznamovať významné narušenia svojich činností. Smernica CER tiež zriadila skupinu pre odolnosť kritických subjektov (CERG), ktorej úlohou je podporovať Komisiu a uľahčovať spoluprácu medzi členskými štátmi a výmenu informácií o otázkach týkajúcich sa tejto smernice, ako sa stanovuje v jej článku 19 ods. 1. Od svojho založenia v januári 2023, keď nadobudla účinnosť smernica CER, sa CERG stretla 13-krát, počas čoho sa uskutočnili dôležité činnosti, najmä prijatie rokovacieho poriadku CERG konsenzom, diskusie o stave transpozície smernice CER na vnútroštátnej úrovni a právny výklad smernice CER, konzultácie v súvislosti s prijatím nariadenia Komisie, ktorým sa ustanovuje zoznam základných služieb, pridanie dvoch krajín Európskeho hospodárskeho priestoru ako pozorovateľov (Island a Nórsko), organizácia prvého spoločného zasadnutia CERG a skupiny pre spoluprácu v oblasti NIS v novembri 2023, ako sa stanovuje v smernici o CER, prezentácie hodnotenia hrozieb pre kritickú infraštruktúru v EÚ v utajenom režime, diskusie zamerané na konkrétne sektory, ako je vesmír, alebo iné prierezové témy, ako je prispôsobenie sa zmene klímy a cezhraničné hodnotenia rizík a diskusie o záťažových testoch kritickej infraštruktúry.

Súčasne sa vytvoria predpoklady pre včasné prijímanie a realizáciu opatrení na posilnenie odolnosti kritických subjektov, zefektívni sa informačný a komunikačný systém pri riadení rizík, pri ich riešení a tiež sa vytvorí a centrálne zabezpečí jednotný a koordinovaný spôsob spravovania rizík a incidentov na úseku kritickej infraštruktúry.

Funkčnosť bezpečnostného systému na úseku kritickej infraštruktúry je potrebné nepretržite zdokonaľovať v súlade s vývojom bezpečnostného prostredia. Navrhované opatrenia sa realizujú prostredníctvom plnenia úloh, napríklad podľa § 15 zákona o kritickej infraštruktúre ústredný orgán na úseku kritickej infraštruktúry môže uskutočniť po vzájomnej dohode uskutočniť najmenej raz ročne koordinačnú poradu s kritickými subjektami vo svojej pôsobnosti s cieľom výmeny informácií a skúsenosti. Ústredné orgány budú informovať o záveroch z týchto porád MV SR alebo skupinu v prípade potreby ďalšieho riešenia.

Úloha	Popis úlohy	Zodpovedný subjekt	Súčinný subjekt	Časový horizont realizácie
č. 8	Budovať bezpečnostnú komunitu v sektoroch kritickej infraštruktúry.	MV SR, MH SR, MD SR, MIRRI SR, SŠHR SR, MZ SR, MŽP SR, MPRV SR	MO SR, SIS, NBÚ, MF SR, kritické subjekty okrem výnimiek podľa § 19 ods. 3 zákona o kritickej infraštruktúre.	Najmenej 1x ročne.

Na zabezpečenie jednotného postupu pri vyhotovovaní hlásení o kontrole je kľúčové vytvorenie spoločnej šablóny, ktorú poskytne MV SR. Táto šablóna bude navrhnutá tak, aby bola prehľadná, komplexná a umožňovala efektívne spracovanie a vyhodnocovanie informácií. Používanie spoločnej šablóny zabezpečí, že všetky kontrolné správy budú obsahovať relevantné a porovnateľné informácie, čo uľahčí centrálne vyhodnocovanie a riadenie rizík kritickej infraštruktúry na úrovni štátu. So závermi z kontrol sa bude zaoberať skupina a tieto závery budú súčasťou úlohy č. 6 vo vyhodnotení správy o bezpečnostnej situácii na úseku kritickej infraštruktúry.

Úloha	Popis úlohy	Zodpovedný subjekt	Súčinný subjekt	Časový horizont realizácie
č. 9	Vytvoriť jednotnú šablónu pre hlásenie o kontrole v kritických subjektoch.	MV SR	MO SR, SIS	December 2026

Nevyhnutným predpokladom kvalitného fungovania bezpečnostného výskumu v podmienkach SR je spolupráca s ďalšími inštitúciami a štátmi v rámci EÚ. Terminologický slovník krízového riadenia a zásady jeho používania vytvára spracovateľom strategických, koncepčných a plánovacích dokumentov a právnych noriem, vedeckým a vzdelávacím inštitúciám podmienky na zjednotenie výkladu termínov a prekladu anglických výrazov do slovenského jazyka a podmienky na ustálenie zásad používania termínov v oblasti bezpečnosti štátu a krízového riadenia v podmienkach SR. Úlohou vedy a výskumu na úseku kritickej infraštruktúry by mal byť

rozvoj teoretických poznatkov a ich šírenie v praxi v procese budovania odolnosti kritickej infraštruktúry. Vedecko-výskumné úlohy na tomto úseku sa odporúčajú spracovávať formou riešiteľských kolektívov z akademickej obce a rôznymi grantovými agentúrami.

V úlohe č. 10 sa navrhuje aktualizácia terminologického slovníka. Vedeckí a pedagogickí pracovníci verejných vysokých škôl spolu s pracovníkmi štátnych vysokých škôl a vedeckých ústavov Slovenskej akadémie vied by mali vedieť participovať pri tvorbe koncepčných materiálov bezpečnostného systému Slovenskej republiky vrátane tých, ktoré sa týkajú kritickej infraštruktúry.

Úloha	Popis úlohy	Zodpovedný subjekt	Súčinný subjekt	Časový horizont realizácie
č. 10	Zabezpečiť aktualizáciu Terminologického slovníka krízového riadenia a zásady jeho používania (2017).	ÚV SR	MO SR, SIS, MV SR, MH SR, MD SR, MIRRI SR, SŠHR SR, NBÚ, MF SR, MŽP SR, MPRV SR, MZ SR, Akademická obec a výskumné inštitúcie	Do 31. decembra 2030

Ďalšou úlohou je vytvoriť a presadiť spoločné, minimálne bezpečnostné štandardy a technické požiadavky pre všetky kritické subjekty v sektoroch, vrátane bezpečnostných štandardov pre fyzickú bezpečnosť digitálnej infraštruktúry. Tieto štandardy by mali zahŕňať ochranu najcitlivejšej infraštruktúry a informácií (bezpečnosť životne dôležitých činností, kybernetická bezpečnosť, ochrana utajovaných skutočností, ochrana vedeckých a technických aktív), ďalej ochranu proti výpadkom energií a tiež aj ochranu pred prírodnými hrozbami.

Úloha	Popis úlohy	Zodpovedný subjekt	Súčinný subjekt	Časový horizont realizácie
č. 11	Vypracovať odporúčania pre minimálne opatrenia na zabezpečenie odolnosti kritických subjektov.	MV SR, MH SR, MD SR, MIRRI SR, SŠHR SR, NBÚ, MF SR, MŽP SR, MPRV SR,	MO SR, SIS, ÚV SR, kritické subjekty, akademická obec a výskumné inštitúcie	Do 31.decembra 2030

Štandardy formou odporúčaní (ďalej len „odporúčanie“) poskytnú základné informácie o organizačných a technických aspektoch ochrany kritickej infraštruktúry vyplývajúcich z ustanovení článku 13 smernice CER a noriem o odolnosti kritických subjektov podľa článku 4 smernice CER. Budú slúžiť ako súbor konkrétnych usmernení pre výstavbu, organizáciu alebo prevádzku systému ochrany.

Odporúčanie[20] identifikuje, do akej miery súvisí ochrana kritickej infraštruktúry s úlohami v oblasti kontinuity poskytovania základných služieb, kybernetickej bezpečnosti, ale aj osobnej, fyzickej, technickej a právnej bezpečnosti, ako aj s cieľmi kritických subjektov a ich zdrojmi. Taktiež môže slúžiť ako zdroj referenčných informácií pre vytvorenie jednej alebo viacerých bezpečnostných politík kritických subjektov, odborných štúdií, ktoré sú zdrojom poznatkov pre zodpovedné osoby na úseku kritickej infraštruktúry, ako aj pre zainteresované strany, t. j. fyzické a právnické osoby, subjekty, služby verejnej bezpečnosti a všeobecnej bezpečnosti, ktoré sa priamo alebo nepriamo podieľajú na ochrane kritickej infraštruktúry.

Odporúčanie je určené pre kritické subjekty, kontaktné osoby systémov kritickej infraštruktúry a zainteresované strany vykonávajúce úlohy kritickej infraštruktúry, ako aj pre tých, ktorí majú záujem o implementáciu vybraných aspektov bezpečnosti kritickej infraštruktúry vo svojich organizáciách.

V rámci riadenia kontinuity činností sa ako opatrenie na základe odporúčania môžu vypracovať sektorové špecifikácie pre riadenie kontinuity činností (Business Continuity Management – BCM), Plán kontinuity činností (Business Continuity Plan - BCP) a Plán obnovy činností (Disaster Recovery Plan – DRP) ako súčasť bezpečnostného plánu. Plán kontinuity činností (BCP) v subjekte predstavuje súhrn konkrétnych činností, ktoré sa budú vykonávať v prípade incidentu na úseku kritickej infraštruktúry. Účelom je zachovanie kontinuity poskytovania základnej služby vykonávania funkcií a úloh v prípade incidentu. BCP upravuje procesy havarijného plánovania a obnovy prevádzky základných služieb po výskyte incidentu na úseku kritickej infraštruktúry. Definuje a odporúča možnosti kritického subjektu a jej zamestnancov tak, aby bolo možné prevádzku základných služieb obnoviť v požadovanom rozsahu a čase na rýchle zvládnutie akéhokoľvek incidentu a zabezpečiť kontinuitu činností.“ Účelom odporúčania uvedených plánov je zachovanie kontinuity poskytovania základných služieb v požadovanom rozsahu a čase, pri koordinovanom riadení naprieč sektorovými väzbami, čím sa vytvára základ pre jednotný systém odolnosti štátu.

Odolnosť kritickej infraštruktúry formuje množstvo právnych a vykonávacích predpisov, koncepcií a stratégií, ktoré predstavujú formálny základ prístupu k budovaniu a zvyšovaniu odolnosti aj na úseku kritickej infraštruktúry. Zoznam relevantných strategických dokumentov podľa sektorov poukazuje na stanovenie štandardov na zabezpečenie kontinuity prevádzkovania základných služieb, ktoré musia sledovať súčasné trendy a koncepcie v bezpečnostnej politike SR (prehľad je uvedený v Prílohe č. II).

[20] Napríklad § 6 písm. i) a § 15 ods. 2 zákona o kritickej infraštruktúre.

4. PODPORA KRITICKÝCH SUBJEKTOV A OPATRENÍ NA POSILNENIE SPOLUPRÁCE MEDZI VEREJNÝM SEKTOROM A SÚKROMNÝM SEKTOROM

Na zabezpečenie efektívneho fungovania stratégie je potrebné zaviesť nielen štandardizované procesy, ale aj podporovať silné partnerstvá. V prvom rade sa navrhuje zabezpečiť aktívnu účasť na podporných programoch zameraných na rozvoj kapacít, budovanie odborných zručností a zvyšovanie úrovne celkovej odolnosti, s dôrazom na využívanie dostupných finančných nástrojov EÚ. Úlohou je iniciovať a koordinovať prípravu projektových zámerov, zapájať sa do partnerských konzorcií a efektívne využívať pridelené zdroje na dosahovanie strategických cieľov v oblasti odolnosti kritických subjektov SR.

Ďalej sa navrhuje maximalizovať pridanú hodnotu finančnej podpory EÚ prostredníctvom udržateľného využívania výsledkov projektov a ich integrácie do prevádzkových a strategických procesov kritických subjektov.

S cieľom spracovania analýzy potrieb (a s tým súvisiacich výdavkov) v súvislosti so zabezpečením odolnosti kritických subjektov, budú ústredné orgány štátnej správy na úseku kritickej infraštruktúry, spolu s MV SR, komunikovať so súkromným sektorom v rámci úlohy č. 8. Kritické subjekty majú v zmysle §10 ods. 1 písm. b) zákona o kritickej infraštruktúre povinnosť chrániť kritickú infraštruktúru. Pri zabezpečovaní tejto povinnosti sa im odporúča aktívne vyhľadávať možnosti financovania svojej odolnosti z finančných nástrojov EÚ a prihlasovať sa na vyhlásené výzvy na národnej ako aj európskej úrovni. V rámci spolupráce a partnerstva vyplývajúcej z úlohy č. 8, môžu byť kritické subjekty informované zo strany ústredného orgánu štátnej správy o vyhlásených výzvach na národnej ako aj európskej úrovni.

V rámci prípravy Národného a regionálneho partnerského plánu (NRPP) pre programové obdobie 2028-2034 bude MV SR informovaná o plánovaných investíciách v oblasti kritickej infraštruktúry zo strany gestorov a spolugestorov [21] pre prípravu NRPP v rámci ich vecnej pôsobnosti, aby bola podľa možnosti téma odolnosti kritických subjektov a ochrany kritickej infraštruktúry zohľadňovaná pri plánovaných investíciách v NRPP.

Čo sa týka implementácie programového obdobia 2028-2034, odporúča sa priamo vo výzvach týkajúcich sa kritickej infraštruktúry usmerniť kritické subjekty, aby v rámci plánovaných výdavkov projektov boli zahrnuté aj výdavky súvisiace so zabezpečením odolnosti (s prihliadnutím na sektorové špecifikácie vrátane výdavkov na organizačné, technické a bezpečnostné opatrenia ako aj na mechanické zábranné prostriedky, technické zabezpečovacie prostriedky, kamerové systémy, bezpečnostné prvky informačných systémov a pod. sektorové špecifikácie) tak, aby bola v rámci modernizácie kritickej infraštruktúry z európskych zdrojov budovaná aj jej odolnosť rešpektujúc špecifické pravidlá doby udržateľnosti modernizačných procesov bezpečne realizovať havarijné zásahy.

Zámerom je zriadenie dotačných schém, ktoré by finančne podporovali kritické subjekty pri modernizácii ich bezpečnostných systémov a technológií a zároveň by riešili potrebu väčšej

[21] Podľa uznesenia vlády SR č. 546 z 5. novembra 2025.

flexibility pri riadení podpory Únie, vrátane silnejšej orientácie na výkonnosť, ako aj väčšie zjednodušenie pre všetky subjekty zapojené do jej vykonávania.

Proces zvyšovania odolnosti kritických subjektov sa opiera o synergie a súdržnosť s príslušnými programami EÚ, najmä k programu Horizont Európa (Horizon Europe), Fondu pre vnútornú bezpečnosť (ISF), a viaže sa aj k iným programom, ktoré sa vzťahujú na príslušné európske priemyselné odvetvia a občiansku spoločnosť, napríklad Program pre jednotný trh a program Digitálna Európa.

5. ŠPECIFICKÉ POSTAVENIE SEKTORA FINANCIE NA ÚSEKU KRITICKEJ INFRAŠTRUKTÚRY

Sektor Financie predstavuje jeden zo strategických pilierov kritickej infraštruktúry SR. Jeho význam spočíva v zabezpečovaní stability platobného a kapitálového trhu, fungovania bánk a finančných inštitúcií, ako aj infraštruktúry finančného trhu a riadenia verejných financií. Európska legislatíva stanovuje špecifické povinnosti, ktoré sa odlišujú od ostatných sektorov kritickej infraštruktúry, čo je dôvodom osobitného postavenia sektora Financie.

Sektor Financie zohráva kľúčovú úlohu v stabilite národného hospodárstva a je úzko prepojený s ostatnými sektormi kritickej infraštruktúry. Je tvorený troma podsektormi Bankovníctvo, Finančné trhy a Systémy riadenia verejných financií, viď príloha č. 1 k zákonu o kritickej infraštruktúre. Na všetky tri podsektory je uplatnená výnimka z plnenia povinností zákona o kritickej infraštruktúre, pričom prvé dva podliehajú osobitným požiadavkám digitálnej prevádzkovej odolnosti podľa Nariadenia Európskeho parlamentu a Rady (EÚ) 2022/2554 zo 14. decembra 2022 o digitálnej prevádzkovej odolnosti finančného sektora a o zmene nariadení (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014, (EÚ) č. 909/2014 a (EÚ) 2016/1011 (ďalej len „nariadenie DORA“) a podsektor Systémy riadenia verejných financií spadá pod reguláciu zákona č. 69/2018 Z. z.

Ak by subjekty finančného sektora museli súčasne plniť povinnosti podľa zákona o kritickej infraštruktúre aj podľa osobitných európskych predpisov, dochádzalo by k duplicite najmä v oblastiach riadenia rizík, plánovania kontinuity, testovania odolnosti a incident reportingu. Zavedená výnimka sleduje princíp „**jedna požiadavka – jeden dôkaz**“, t. j. povinnosti splnené podľa nariadenia DORA, alebo podľa zákona č. 69/2018 Z. z. sa považujú za splnené aj pre rámec zákona o kritickej infraštruktúry.

Dohľad nad časťou finančného sektorom v oblasti digitálnej odolnosti vykonáva NBS v súlade s nariadením DORA a usmerneniami európskych orgánov dohľadu (EBA, ESMA, EIOPA). Výnimka preto umožňuje, aby dohľad nad sektorom Financie vykonávali orgány s príslušnou odbornosťou a mandátom, čím sa predchádza duplicite procesov.

Ustanovená výnimka neznamená, že sektor Financie stráca postavenie na úseku kritickej infraštruktúry. Naďalej zostáva kritickým sektorom podľa smernice CER aj podľa zákona o kritickej infraštruktúre, avšak jeho povinnosti sa plnia prostredníctvom špecifických sektorových rámcov (DORA, NIS 2). Tým sa zabezpečuje vysoká úroveň ochrany a zároveň sa predchádza zbytočnej administratívnej záťaži.

Pre zabezpečenie odolnosti sektora Financie je preto nevyhnutná efektívna a účinná spolupráca subjektov dohľadu.

Úloha	Popis úlohy	Zodpovedný subjekt	Súčinný subjekt	Časový horizont realizácie
č. 13	Vytvoriť pracovnú skupinu pre sektor „Financie“	MF SR	NBS	Do 31. marca 2026

Implementáciou tejto stratégie sa posilní schopnosť bánk, finančných inštitúcií a systému riadenia verejných financií čeliť narušeniam, obnoviť prevádzku a zabezpečiť kontinuitu kľúčových služieb v súlade s legislatívnymi požiadavkami.

6. ZOZNAM ORGÁNOV ŠTÁTNEJ SPRÁVY A PRÍSLUŠNÝCH ZAINTERESOVANÝCH STRÁN ZAPOJENÝCH DO VYKONÁVANIA STRATÉGIE

Stratégiu vypracovalo Ministerstvo vnútra SR na základe § 5 písm. a) v spojení s § 7 zákona o kritickej infraštruktúre. Vzhľadom nato, že kritická infraštruktúra je v SR prierezová agenda v pôsobnosti viacerých ústredných orgánov štátnej správy podľa § 3 písm. c) zákona o kritickej infraštruktúre, na príprave stratégie spolupracovali aj Ministerstvo hospodárstva SR, Ministerstvo financií SR, Ministerstvo investícií, regionálneho rozvoja a informatizácie SR, Ministerstvo dopravy SR, Ministerstvo životného prostredia SR, Ministerstvo zdravotníctva SR, Ministerstvo pôdohospodárstva a rozvoja vidieka SR, Národný bezpečnostný úrad a Správa štátnych hmotných rezerv SR.

Vzhľadom na špecifické postavenie subjektov digitálneho sektora a finančného sektora sa na plnení stratégie podieľajú dotknuté ÚOŠS SR iba v takom rozsahu, v akom kritické subjekty majú povinnosti podľa zákona o kritickej infraštruktúre.

S cieľom ísť nad rámec ochrany kritickej infraštruktúry a všeobecnejšie zabezpečiť odolnosť kritických subjektov prevádzkujúcich kritickú infraštruktúru, ktoré poskytujú základné služby na trhu, je potrebné zapojiť do vykonávania stratégie aj KBR SR.

Bezpečnostné informácie sú kľúčové pre včasné varovanie a reakciu na hrozby a preto do systému vykonávania stratégie vstupujú aj subjekty zodpovedné za ich zber, analýzu a operatívne využitie:

- SIS (vrátane NBAC) a Vojenské spravodajstvo (vrátane Centra kybernetickej obrany) - zodpovedajú za zber a analýzu spravodajských informácií.
- Policajný zbor SR - rieši trestnoprávne aspekty kriminality, zabezpečuje verejný poriadok a bezpečnosť.

Cieľom stratégie je výmena informácií[22] s týmito zložkami o hrozbách a potenciálnych rizikách. Táto spolupráca je nevyhnutná na vytvorenie komplexného situačného povedomia a na včasnú identifikáciu proti pokročilých pretrvávajúcich kybernetických hrozieb (APT), vrátane štátom podporovaných aktérov, ktoré ako dlhodobé, cielené a technicky sofistikované pôsobenie môžu zásadným spôsobom ohroziť kritické subjekty a ich kritickú infraštruktúru.

Ďalší dôležitý bod zapojenia predstavuje akademická spolupráca. Tento dôležitý zdroj predstavuje inovácie, výskum a expertízne znalosti, ktoré sú kľúčové pre pochopenie nových hrozieb a vývoj moderných metód zvyšovania odolnosti. Poskytovanie základných služieb je neustály proces, ktorý si vyžaduje budovanie znalostných kapacít, preto do stratégie sú zapojení aj akademický sektor, výskumné inštitúcie a záujmové združenia právnických osôb.

[22] Podľa § 38 zákona č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov.

7. OPIS ZAVEDENÝCH OPATRENÍ, KTORÉ SÚ ZAMERANÉ NA UĽAHČENIE VYKONÁVANIA POVINNOSTÍ MALÝMI A STREDNÝMI PODNIKMI, KTORÉ SÚ IDENTIFIKOVANÉ AKO KRITICKÉ SUBJEKTY

Celkovo je proces zabezpečenia odolnosti kritickej infraštruktúry komplexným úsilím, ktoré si vyžaduje neustálu aktualizáciu a prispôsobovanie sa meniacim sa bezpečnostným hrozbám. Kritický subjekt spolu s ústrednými orgánmi musí neustále monitorovať vyvíjajúcu sa situáciu a byť pripravený aktualizovať potrebné bezpečnostné opatrenia na zabezpečenie ochrany kritickej infraštruktúry a predchádzať prípadným incidentom s cieľom zvyšovania celkovej odolnosti. Pri odporúčaní minimálnych opatrení na zabezpečenie odolnosti kritického subjektu ústredným orgánom podľa § 6 písm. i) zákona o kritickej infraštruktúre budú ústredné orgány dbať o primerané prehlbovanie povinností len vo vzťahu k jeho kritickej infraštruktúre z dôvodu zabezpečenia odolnosti kritickej infraštruktúry a zabezpečenia poskytovania základnej služby.

Ak už kritický subjekt uskutočnil iné posúdenia rizika alebo vypracoval dokumenty na plnenie povinností podľa osobitných predpisov[23], ktoré sú relevantné pre jeho posúdenie rizika kritickým subjektom, môže tieto posúdenia a dokumenty použiť na splnenie požiadaviek ustanovených v zákone o kritickej infraštruktúre. Ústredný orgán môže vyhlásiť takéto posúdenie rizika uskutočnené kritickým subjektom, ktoré sa zaoberá rizikami a mierou závislosti, za úplne alebo čiastočne v súlade s povinnosťami podľa zákona o kritickej infraštruktúre. Ak ústredný orgán posúdenie rizika nevyhlási za súladné s povinnosťami, oznámi kritickému subjektu, že je povinný vykonať posúdenie rizika kritickým subjektom, a určí na to primeranú lehotu, ktorá nemôže byť kratšia ako šesť mesiacov a dlhšia ako deväť mesiacov v zmysle § 11 ods. 3 zákona o kritickej infraštruktúre.

Ochranu prvkov kritickej infraštruktúry upravuje zákon č. 45/2011 Z. z., ktorý platí v prechodnom období až do procesu identifikácie nových kritických subjektov jednotlivými ústrednými orgánmi (najneskôr do 17.7.2026). Zákon č. 367/2024 Z. z. zásadným spôsobom mení legislatívnu úpravu ochrany kritickej infraštruktúry, pričom aplikácia nového zákona je podmienená schválením predloženej stratégie a kritérií významnosti[24] vládou SR. V tomto časovo vymedzenom tzv. prechodnom období trvá povinnosť zabezpečiť ochranu prvkov kritickej infraštruktúry podľa § 9 zákona č. 45/2011 Z. z. rešpektujúc pritom ustanovenia § 13 a § 21 zákona č. 367/2024 Z. z.

[23] Napríklad § 18 ods. 1 písm. b) zákona č. 319/2002 Z. z. o obrane Slovenskej republiky v znení zákona č. 306/2019 Z. z., § 7 ods. 5, príloha č. 1 bod B. písm. f), bod C. písm. k) a bod D. písm. f) zákona č. 541/2004 Z. z. v znení neskorších predpisov, § 10 zákona č. 128/2015 Z. z., zákon č. 69/2018 Z. z. v znení neskorších predpisov, zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

[24] Kritériá významnosti vplyvu na určenie kritických subjektov a kritických subjektov osobitného európskeho významu pre každý sektor a podsektor a pre každú základnú službu podľa prílohy č. 1 zákona č. 367/2024 Z. z. o kritickej infraštruktúre a o zmene a doplnení niektorých zákonov. Pozri uznesenie vlády SR k stratégii odolnosti kritických subjektov úloha B3.

8. SPOLUPRÁCA A MEDZINÁRODNÍ PARTNERI

SR je demokratický a právny štát, ktorý dodržiava princípy základných práv a slobôd. Preto sa pri medzinárodnej spolupráci v oblasti odolnosti kritických subjektov zameriava na politickú a technickú spoluprácu so štátmi a medzinárodnými organizáciami, ktoré rešpektujú a presadzujú rovnaké hodnoty.

Odolnosť kritickej infraštruktúry predstavuje kľúčový prvok národnej a medzinárodnej bezpečnosti v dnešnom komplexnom bezpečnostnom prostredí. SR si plne uvedomuje túto skutočnosť a aktívne sa zapája do medzinárodných mechanizmov zameraných na cvičenia a záťažové testovanie kritických subjektov, ktoré posilnia odolnosť a pripravenosť na zvládanie hrozieb pre zachovanie životne dôležitých spoločenských funkcií, hospodárskych činností, verejného zdravia, bezpečnosti alebo životného prostredia a na vnútornom trhu EÚ.

Spolupráca v rámci Európskej únie

SR ako člen EÚ sa v oblasti ochrany kritickej infraštruktúry podieľa na práci v rámci stálych pracovných skupín EÚ. Zvlášť dôležitá je jej účasť v skupinách ako je skupina pre odolnosť kritických subjektov (CERG[25] zriadená na základe článku 19 smernice CER) a pracovná skupina Rady EÚ pre civilnú ochranu v konfigurácii pre odolnosť kritických subjektov (PROCIV CER), ktoré sa zameriavajú na koordináciu politík, zdieľanie osvedčených postupov a rozvoj opatrení potrebných na zvýšenie odolnosti kritickej infraštruktúry. SR je pripravená rozširovať spoluprácu s ostatnými členskými štátmi Európskeho hospodárskeho priestoru. Cieľom je nielen zdieľanie informácií a skúseností, ale aj vytváranie synergických efektov pri riešení cezhraničných hrozieb a budovaní spoločnej odolnosti. Táto spolupráca sa odvíja od princípu zodpovednosti za bezpečnosť a odolnosť vlastných základných služieb, pretože hrozby môžu ovplyvniť fungovanie celého vnútorného trhu EÚ, najmä v kontexte rastúcej vzájomnej závislosti medzi sektormi vnútri štátu aj cezhranične.

Spolupráca v rámci NATO

V oblasti obrany je SR viazaná členstvom v NATO, ktoré kladie veľký dôraz na ochranu kritickej infraštruktúry, pretože jej narušenie môže mať priamy dopad na kolektívnu obranu a schopnosti reagovať na krízy. Cieľom je zabezpečiť, aby kritická infraštruktúra členských štátov bola dostatočne chránená pred rôznymi hrozbami a aby bola zabezpečená jej funkčnosť aj v krízových situáciách. V tejto nadväznosti sa odporúča úzka spolupráca SR s NATO prostredníctvom odborných zástupcov ÚOŠS SR v pracovných skupinách a vo výboroch NATO.

Spolupráca v rámci súkromného sektora a akademickej obce

Zvyšovanie odolnosti kritických subjektov si vyžaduje úzke prepojenie nielen medzi štátnymi inštitúciami, ale aj s tými, ktorí infraštruktúru priamo prevádzkujú a spravujú – súkromným sektorom – a s tými, ktorí prinášajú nové poznatky a inovatívne riešenia – akademickou obcou.

[25] Skupina pre odolnosť kritických subjektov zasadá pravidelne a v každom prípade aspoň raz ročne sa schádza so skupinou NIS pre spoluprácu zriadenou (podľa smernice (EÚ) č. 2022/2555) s cieľom podporovať a uľahčovať spoluprácu a výmenu informácií.

Zapojenie súkromného sektora

Súkromný sektor zohráva v oblasti kritickej infraštruktúry nezastupiteľnú úlohu, preto je nevyhnutné budovať silné partnerstvá a mechanizmy spolupráce, ktoré zabezpečia efektívnu výmenu informácií o potenciálnych hrozbách, rizikách a incidentoch. To zahŕňa pravidelné dialógy, spoločné cvičenia a iniciovanie opatrení ako súčasť strategického cieľa č. 3: Komplexný prístup k odolnosti. Realizácia navrhovaných opatrení však nesmie neprimeraným spôsobom zaťažovať podnikateľské subjekty, ktoré budú identifikované ako kritické subjekty.

9. ZÁVERY A IMPLEMENTAČNÉ ODPORÚČANIA

Cieľom predkladanej stratégie podľa transponovanej smernice CER v § 7 zákona o kritickej infraštruktúre je stanoviť ciele, so zámerom zvýšiť odolnosť kritických subjektov, a to nielen pokiaľ ide o pripravenosť, ale aj o systém reakcie, koordinácie a posudzovanie informácií o incidentoch a hrozbách. Preto je potrebné definovať a naplánovať tieto dôležité kroky, aby sa dosiahol čo najefektívnejší prístup k budovaniu odolnosti.

Táto stratégia sa vykonáva v súlade s právnym rámcom kybernetickej bezpečnosti podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a jeho vykonávacích predpisov[26].

Hlavnú zodpovednosť za implementáciu, monitorovanie a podávanie správ k Stratégii má MV SR, ktoré má v rámci medzirezortných a prierezových úloh koordinačnú funkciu. Medzirezortná koordinácia na najvyššej úrovni a operatívna koordinácia implementácie bude prebiehať prostredníctvom stálej medzirezortnej skupiny pre kritickú infraštruktúru, ktorej členmi sú nominovaní zástupcovia jednotlivých ÚOŠS SR a spravodajských a bezpečnostných zložiek.

Na úspešnú implementáciu stratégie je potrebné zadefinovať predpoklady zabezpečenia kontinuity realizácie opatrení a úloh ustanovených stratégiou. Stratégia je strednodobý dokument, ktorý sa príjme na obdobie 4 rokov, v prípade zmeny bezpečnostného prostredia alebo iných vplyvov, ktoré by mohli výrazne ovplyvniť fungovanie základných služieb v SR, sa môže dokument aktualizovať aj skôr.

Navrhuje sa, aby podľa § 7 ods. 1 písm. g) zákona o kritickej infraštruktúre skupina pre kritickú infraštruktúru spracovala ročnú správu o vyhodnotení bezpečnostnej situácií na úseku kritickej infraštruktúry, ktorej súčasťou bude aj opis a stav jednotlivých schválených úloh v rámci stratégie.

Pre realizáciu stratégie platí všeobecné pravidlo, že základným spôsobom financovania opatrení naplánovaných stratégiou je ich priame začlenenie do sektorových politík. Druhým pravidlom, na ktoré by sa pri financovaní malo prihliadať, je identifikácia pozitívnych medzisektorálnych synergií a spájanie viacerých finančných zdrojov na realizáciu rozsiahlejších opatrení ako sú napríklad:

- odporúčania pre minimálne opatrenia na zabezpečenie odolnosti kritických subjektov,
- zabezpečenie a implementácia vhodného spôsobu na nahlasovanie incidentov v kritickej infraštruktúre.

Nižšie uvádzame existujúce zdroje na financovanie činností spojených s komplexným riadením rizík bezpečnostných hrozieb:

[26] Najmä vyhlášky Národného bezpečnostného úradu č. 226/2025 Z. z., ktorou sa ustanovujú podrobnosti o hláseniach a vyhláškou Národného bezpečnostného úradu č. 227/2025 Z. z. o bezpečnostných opatreniach), zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a jeho vykonávacích predpisov, ako aj nariadení EÚ - 2016/679 všeobecné nariadenie o ochrane údajov GDPR, 2024/1689 akt o umelej inteligencii, 2023/2854 akt o údajoch, 2022/868 akt o správe údajov a 2024/2847 akt o kybernetickej bezpečnosti.

- každý ústredný orgán realizuje schválené opatrenia v rámci schválených národných plánov rozvoja a plnenia rezortných stratégií,
- v rámci ochrany kritickej infraštruktúry majú príslušné ÚOŠS SR vytvorený medzirezortný rozpočtový program 0AS Ochrana kritickej infraštruktúry v SR.

Okrem štátneho rozpočtu sú ďalšou možnosťou finančných zdrojov programy a fondy EÚ.

Možné zdroje dodatočného financovania:

- štátny rozpočet,
- Program Slovensko,
- bilaterálne programy SR zamerané na vedu a výskum,
- komunitárne programy EÚ: DG ECHO, DG HOME, Horizon Europe a iné, ktoré podporujú činnosti v oblasti vedy, výskumu a inovácií aj z oblasti bezpečnosti a civilnej ochrany,
- iné medzinárodné programy.

ZOZNAM PRÍLOH