NÁRODNÝ
BEZPEČNOSTNÝ
ÚRAD

# Akčný plán realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2021 až 2025

# Obsah

# Úvod

Kybernetická bezpečnosť je s neustále rastúcou digitalizáciou spoločnosti jednou z najdôležitejších oblastí, ktorá priamo ovplyvňuje fungovanie modernej spoločnosti. Aby bolo možné ju efektívne riadiť, potrebuje strategické ukotvenie v systéme správy štátu. Komplexný prístup ku kybernetickej bezpečnosti s jasnými princípmi a cieľmi nie len zaručuje jasnú víziu, ale aj potvrdzuje jej dôležitosť v celom bezpečnostnom systéme.

Previazanie kybernetickej bezpečnosti s problematikou počítačovej kriminality, kybernetického spravodajstva, kybernetickej obrany a kybernetickej diplomacie podčiarkuje multidimenzionálny presah kybernetickej bezpečnosti do viacerých významných oblastí, ktoré formujú kybernetický priestor. Systém riadenia kybernetickej bezpečnosti si na národnej úrovni vyžaduje nie len implementáciu tuzemských právnych noriem a procesov, ale musí zohľadňovať aj vývoj na úrovni EÚ, Rady Európy a OSN, nakoľko problematika kybernetickej bezpečnosti stiera hranice medzi štátmi a má globálny dopad na fungovanie spoločnosti.

Dňa 7. januára 2021 bola vládou schválená Národná stratégia kybernetickej bezpečnosti na roky 2021 až 2025 (ďalej len "Národná stratégia"), ktorá zakotvila smerovanie Slovenskej republiky (ďalej len „SR") v oblasti kybernetickej bezpečnosti. V Národnej stratégii sú popísané princípy, na ktorých stojí systém riadenia kybernetickej bezpečnosti, ako aj hrozby, ktoré vplývajú na procesy a činnosti v oblasti kybernetickej bezpečnosti a majú významný dopad na bezpečnosť štátu, ako aj jeho obyvateľov. Ako reakcia na tieto hrozby Národná stratégia určila strategické ciele, na ktoré je potrebné sa najbližších minimálne 5 rokov zamerať:

1. Dôveryhodný štát pripravený na hrozby
2. Efektívne odhaľovanie a objasňovanie počítačovej kriminality
3. Odolný súkromný sektor
4. Kybernetická bezpečnosť ako základná súčasť verejnej správy
5. Silné partnerstvá
6. Vzdelaní odborníci a vzdelaná verejnosť
7. Výskum a vývoj v oblasti kybernetickej bezpečnosti

Aby mohla byť Národná stratégia a jej ciele vykonateľné, musia byť určené konkrétne úlohy a aktivity spolu s jasnými zodpovednosťami. Na tento účel slúži Akčný plán Národnej stratégie kybernetickej bezpečnosti na roky 2021 až 2025 (ďalej len "Akčný plán"), ktorý tieto úlohy definuje, určuje zodpovedné subjekty a takisto aj časové horizonty pre jednotlivé úlohy.

Cieľom Akčného plánu je vytvoriť ucelený koncept úloh a aktivít v oblasti kybernetickej bezpečnosti na najbližších 5 rokov. Navrhované úlohy sú adekvátne k potrebám naplnenia vízie a strategických cieľov stratégie a rešpektujú základné princípy, ktoré boli v stratégii zakotvené.

Budovanie spôsobilostí v oblasti kybernetickej bezpečnosti je nevyhnutným predpokladom na účinnú ochranu kybernetického priestoru. Ide o komplexný proces, zahŕňajúci budovanie personálnych kapacít, vybudovanie organizačného rámca, rozvíjanie partnerskej spolupráce na národnej a medzinárodnej úrovni ako aj akvizície technických a technologických nástrojov. Vhodné nastavenie

systému budovania spôsobilostí, zahŕňajúceho konkrétne úlohy a aktivity, prinesie jasné priority, ako aj smerovanie SR v oblasti kybernetickej bezpečnosti.

Za monitorovanie implementácie Akčného plánu bude zodpovedný stály monitorovací výbor pre implementáciu Akčného plánu. Za implementáciu úloh a aktivít budú zodpovedné konkrétne subjekty, uvedené pri jednotlivých úlohách a aktivitách Akčného plánu. Súčinnostné subjekty poskytujú zodpovedným subjektom podporu a pomoc pri implementácii.

**Systém riadenia kybernetickej bezpečnosti v SR**

Dňa 1.1.2016 novelou zákona č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy sa Národný bezpečnostný úrad (ďalej len „úrad") stal ústredným orgánom štátnej správy pre kybernetickú bezpečnosť. Úrad tak prevzal zodpovednosť za túto oblasť a tým sa zjednotila kompetencia, súvisiaca so riadením kybernetickej bezpečnosti v Slovenskej republike. Dňom 1. apríla 2018 vstúpil do platnosti zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti, ktorým sa transponovala Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (ďalej len "smernica NIS"), ale najmä precizovalo postavenie, úlohy a právomoci úradu v oblasti kybernetickej bezpečnosti a legislatívne sa zadefinoval a zjednotil systém riadenia kybernetickej bezpečnosti.

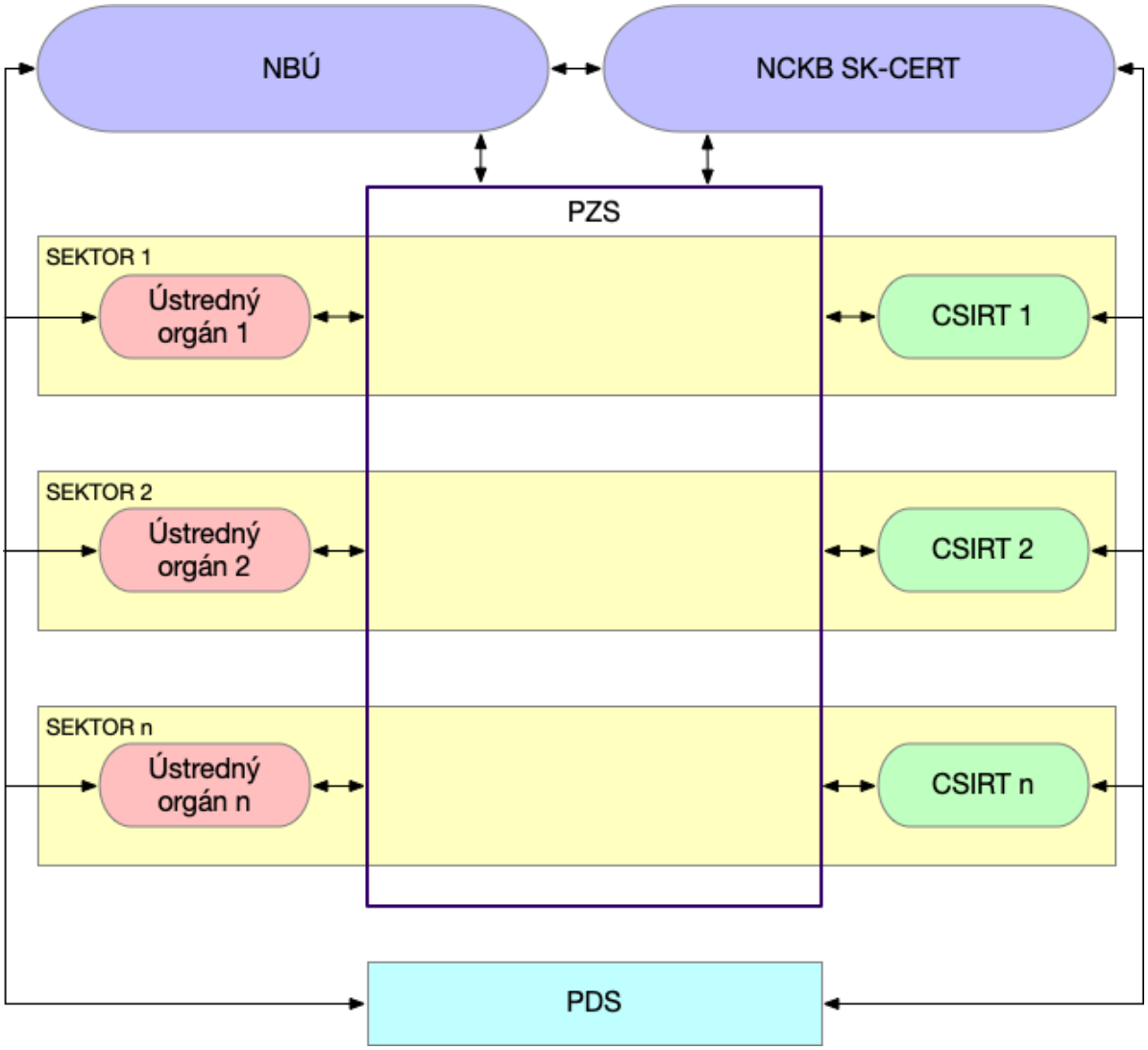
Systém riadenia kybernetickej bezpečnosti v Slovenskej republike má niekoľko vrstiev, ktoré môžeme rozdeliť na národnú úroveň a sektorovú úroveň. Na národnej úrovni úrad riadi strategické, koncepčné a normotvorné činnosti, je kontaktným bodom pre zahraničie vrátane medzinárodných organizácií, vedie register základných služieb, register prevádzkovateľov základných služieb, register poskytovateľov digitálnych služieb a vykonáva ďalšie dôležité činnosti a aktivity v oblasti kybernetickej bezpečnosti na národnej úrovni, vymedzené v §5 zákona o kybernetickej bezpečnosti. Taktiež plní úlohu Národnej jednotky CSIRT, ktorá na národnej úrovni rieši a koordinuje riešenie kybernetických bezpečnostných incidentov, vydáva včasné varovania a výstrahy pred kybernetickými bezpečnostnými incidentami a zraniteľnosťami a rieši ostatné úlohy, súvisiace s riešením kybernetických bezpečnostných incidentov a obnovou systémov.

Na sektorovej úrovni je podľa zákona definovaných 11 sektorov a 25 podsektorov. Za každý zo sektorov je zodpovedný ústredný orgán (ďalej len „ústredný orgán"), ktorý plní úlohy na úrovni poskytovania požadovanej súčinnosti s úradom, spolupráce s inými sektorovými ústrednými orgánmi a prevádzkovateľmi základných služieb vo svojej pôsobnosti, budovaní bezpečnostného povedomia, koordinovanej spolupráce na všetkých stupňoch riadenia kybernetickej bezpečnosti, aplikácie bezpečnostných opatrení, identifikácie základnej služby a prevádzkovateľa základnej služby a spolupráce so zahraničnou inštitúciou obdobného zamerania.

V každom sektore, na základe identifikácie podľa zákona, vystupujú prevádzkovatelia základných služieb. Títo majú povinnosti, vyplývajúce zo zákona a to najmä prijať a dodržiavať zákonne vymedzené bezpečnostné opatrenia, bezodkladne úradu hlásiť závažný kybernetický bezpečnostný incident, riešiť kybernetické bezpečnostné incidenty, zabezpečovať dôkazy o kybernetických bezpečnostných incidentoch, spolupracovať s úradom a ústredným orgánom, ako aj oznámiť orgánom činným v trestnom konaní, ak bol spáchaný trestný čin v súvislosti s kybernetickým bezpečnostným incidentom.

Zákon definuje aj Poskytovateľov digitálnej služby, ktorý prevádzkuje jednu z troch služieb - online trhovisko, internetový vyhľadávač alebo službu v cloud computingu. Ich povinnosti sú veľmi podobné ako povinnosti Prevádzkovateľov základnej služby - teda prijať a dodržiavať bezpečnostné opatrenia v rozsahu špecifickom pre poskytovateľa digitálnej služby, hlásiť kybernetický bezpečnostný incident (podľa špecifických pravidiel) a tento aj riešiť a spolupracovať s úradom pri jeho riešení.

Obrázok nižšie graficky popisuje vzťahy medzi subjektmi riadenia systému kybernetickej bezpečnosti na národnej úrovni.



# Úlohy a aktivity

V prípade, že pri jednej úlohe je viacero zodpovedných subjektov, úlohu plní každý subjekt samostatne v rámci svojich kompetencií a samostatne aj zasiela odpočet plnenia úlohy monitorovaciemu výboru pre implementáciu Akčného plánu; v prípade, ak ide o úlohu pri ktorej je uvedených viacero zodpovedných subjektov a plnenie úlohy je možné len v ich vzájomnej kooperácii posielajú tieto odpočet plnenia úlohy spoločne.

## Všeobecné úlohy k stratégii

| Kód úlohy | Úloha | Popis úlohy | Zodpovedný subjekt | Súčinný subjekt | Časový horizont realizácie |
|---|---|---|---|---|---|
| Z.1 | Zriadenie stáleho monitorovacieho výboru pre implementáciu Akčného plánu | Zriadiť stály monitorovací výbor pre implementáciu Akčného plánu podľa schváleného štatútu, predsedu menuje riaditeľ NBÚ. Členmi budú zástupcovia každého zodpovedného subjektu, ktorý má určenú aspoň jednu úlohu v Akčnom pláne | NBÚ | Zástupcovia zodpovedných subjektov s aspoň jednou úlohou v Akčnom pláne | Do 1 mesiaca po schválení akčného plánu vládou SR |
| Z.2 | Merateľné ukazovatele | Pripraviť merateľné ukazovatele pre každú úlohu akčného plánu a predložiť ich monitorovaciemu výboru na schválenie | Subjekt zodpovedný za aspoň jednu úlohu v akčnom pláne | | Do 6 mesiacov po schválení akčného plánu vládou SR |
| Z.3 | Odpočet plnenia Akčného plánu | Každých 12 mesiacov každý zodpovedný subjekt pripraví správu o plnení akčného plánu za svoje úlohy (s vyhodnotením podľa schválených merateľných ukazovateľov) a túto zašle výboru na schválenie. Správa musí obsahovať aj riziká prípadného nesplnenia jednotlivých úloh | Subjekt zodpovedný za každú úlohu v akčnom pláne | | Priebežne, minimálne každých 12 mesiacov |

| | | | | | |
|---|---|---|---|---|---|
| Z.4 | Vypracovanie pravidelnej ročnej správy o plnení úloh Akčného plánu | Vypracovať priebežnú správu o plnení úloh Akčného plánu a predložiť ho riaditeľovi NBÚ vždy do konca januára zo strany monitorovacieho výboru | Monitorovací výbor | | Priebežne |
| Z.5 | Financovanie úloh | Subjekty zodpovedné za konkrétne všeobecné úlohy k stratégii zabezpečia aj financovanie konkrétnej úlohy Akčného plánu prostredníctvom operačných programov fondov Európskeho spoločenstva, fondu obnovy a iných foriem financovania. | MIRRI SR, MF SR | | Priebežne |

# 1. Dôveryhodný štát pripravený na hrozby

| Kód úlohy | Úloha | Popis úlohy | Zodpovedný subjekt | Súčinný subjekt | Časový horizont realizácie |
|---|---|---|---|---|---|
| A.1 | Novela vyhlášky o identifikačných kritériách | Pripraviť a zabezpečiť schválenie novely vyhlášky. ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby) | NBÚ | Ústredné orgány štátnej správy, PZS, odborná verejnosť, SIS | 12/2021 |
| A.2 | Novela vyhlášky o kategóriách incidentov | Pripraviť a zabezpečiť schválenie novely vyhlášky, ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov | NBÚ | Ústredné orgány, SIS, PZS, VS, odborná verejnosť | 12/2021 |
| A.3 | Politiky | Vytvorenie ekonomického modelu politík v oblasti kybernetickej bezpečnosti v slovenskej republike | NBÚ | SIS, MF SR, MIRRI SR | 12/2022 |
| A.4 | Implementácia NIS 2.0 | Pripraviť novelu zákona o kybernetickej bezpečnosti, a súvisiacich zákonov, ktorá bude implementovať pripravovanú smernicu NIS 2.0, zabezpečiť | NBÚ | Sektorové ústredné orgány, PZS, | Do 12 mesiacov od schválenia |

| | | | | | |
|---|---|---|---|---|---|
| | | predloženie novely do parlamentu | | odborná verejnosť | smernice |
| A.5 | Posúdenie rizík | Pripraviť metodiku posúdenia rizík pre aplikovanie na sektory štátu, vybrané nové technológie, služby s cieľom poznať možné bezpečnostné dopady na základné a kritické aktíva štátu, prevádzkovateľov základných služieb a občanov. | NBÚ | SIS, Sektorové ústredné orgány | 6/2022 |
| A.6 | Prvé posúdenie rizík | Vykonať prvé sektorové posúdenie rizík | NBÚ | Sektorové ústredné orgány | 12/2022 |
| A.7 | Priebežné posúdenie rizík | Najmenej jedenkrát ročne aktualizovať sektorové posúdenie rizík | NBÚ | Sektorové ústredné orgány | 12/2022 a následne raz ročne |
| A.8 | Sektorové vyhlášky | Pripraviť všeobecne záväzný právny predpis, ktorým sa ustanovia sektorové bezpečnostné opatrenia pre každý sektor (podsektor) podľa zákona o kybernetickej bezpečnosti | Sektorové ústredné orgány | NBÚ | 12/2022 |
| A.9 | Analytické pracovisko | Posilniť analytické kapacity v oblasti bezpečnostných hrozieb, posúdenia rizík, analýz vplyvov, bezpečnostných modelov a dátovej analytiky | NBÚ | | 12/2021 |
| A.10 | Detekcia a zber | Rozvíjať schopnosti v oblasti detekcie a zberu bezpečnostne relevantných udalostí v národnom kybernetickom priestore, ako aj rozvíjať schopnosti v oblasti vyhodnocovania udalostí a detekcie incidentov modernými technikami v národnom kybernetickom priestore rôznymi formami, algoritmami a technológiami, vrátane umelej inteligencie | NBÚ | SIS, VS, MIRRI SR | Priebežne |
| A.11 | Atribúcia | Vytvoriť proces technickej a politickej atribúcie incidentov spolu s určením zodpovedných inštitúcií a právnych mechanizmov a mechanizmov kybernetickej diplomacie | NBÚ | MO SR, SIS, MZVEZ SR | 12/2021 |

| | | | | | |
|---|---|---|---|---|---|
| A.12 | Varovania | Priebežne vytvárať a zverejňovať varovania pred technologickými zraniteľnosťami a problematickými aktivitami v kybernetickom priestore, vrátane adresných varovaní konkrétnym subjektom | NBÚ | | Priebežne |
| A.13 | Verejnosť | Zúčastňovať sa, prezentovať a diskutovať s odbornou verejnosťou aktuálne výzvy, problémy a riešenia v oblasti kybernetickej bezpečnosti - na pracovných stretnutiach, workshopoch, konferenciách a okrúhlych stoloch | NBÚ, sektorové ústredné orgány | | Priebežne |
| A.14 | CSIRT | Podporovať vznik špecializovaných pracovísk typu CSIRT na území SR | NBÚ | | Priebežne |
| A.15 | Budovanie spôsobilostí v oblasti obrany | Pokračovať v budovaní, nastavovaní, posilňovaní a udržiavaní plnohodnotných spôsobilostí kybernetickej bezpečnosti rezortu obrany pre potreby adekvátneho zabezpečenia existujúcej a perspektívnej informačnej a komunikačnej infraštruktúry, ako aj novo zavádzaných zbraňových systémov | MO SR | | Priebežne |
| A.16 | | Inkorporovať do procesov národného obranného plánovania fixné organizačné, personálne a finančné vyčlenenie zdrojov potrebných na budovanie, rozširovanie a udržiavanie rezortných spôsobilostí na zabezpečenie kybernetickej bezpečnosti existujúcej a perspektívnej informačnej a komunikačnej infraštruktúry, ako aj novo zavádzaných zbraňových systémov | MO SR | | 12/2022 |
| A.17 | Budovanie spôsobilostí v oblasti spravodajstva | Pokračovať v budovaní, nastavovaní, posilňovaní a udržiavaní plnohodnotných spôsobilostí kybernetického spravodajstva, zlepšovať technické aj personálne spôsobilosti. | SIS | NBÚ, VS | Priebežne |
| A.18 | Zavedenie systému manažérstva informačnej bezpečnosti | Implementovať systém manažérstva informačnej bezpečnosti u orgánov riadenia v zmysle zákona č. 95/2019 Z. z., od ktorých sa vyžadujú bezpečnostné | MIRRI SR | | 10/2025 |

| | | | | | |
|---|---|---|---|---|---|
| | | opatrenia kategórie II alebo kategórie III podľa vyhlášky č. 179/2020 Z. z. | | | |
| A.19 | | Implementovať systém manažérstva informačnej bezpečnosti u PZS v zmysle zákona č. 69/2018 Z. z., od ktorých sa vyžadujú bezpečnostné opatrenia kategórie II alebo kategórie III podľa vyhlášky č. 362/2018 Z. z. | NBÚ | | 10/2025 |
| A.20 | Certifikácia systému manažérstva informačnej bezpečnosti | Certifikovať integrované systémy manažérstva kvality, manažérstva informačnej bezpečnosti, manažérstva IT služieb a manažérstva kontinuity činností, podľa normy STN EN ISO/IEC 17021 u orgánov riadenia v zmysle zákona č. 95/2019 Z. z., od ktorých sa vyžadujú bezpečnostné opatrenia kategórie II alebo kategórie III podľa vyhlášky č. 179/2020 Z. z. | MIRRI SR | orgány posudzova-nia zhody | 10/2025 |
| A.21 | | Certifikovať integrované systémy manažérstva kvality, manažérstva informačnej bezpečnosti, manažérstva IT služieb a manažérstva kontinuity činností, podľa normy STN EN ISO/IEC 17021 u PZS v zmysle zákona č. 69/2018 Z. z., od ktorých sa vyžadujú bezpečnostné opatrenia kategórie II alebo kategórie III podľa vyhlášky č. 362/2018 Z. z. | NBÚ | orgány posudzova-nia zhody | 10/2025 |
| A.22 | Certifikácia výrobkov, procesov a služieb v oblasti kybernetickej bezpečnosti | Akreditovať KCCKB pre posudzovanie zhody výrobkov, procesov a služieb v oblasti kybernetickej bezpečnosti podľa osobitného predpisu a podľa normy STN EN ISO/IEC 17065 „Posudzovanie zhody. Požiadavky na orgány vykonávajúce certifikáciu výrobkov, procesov a služieb (ISO/IEC 17065)“ | KCCKB | SNAS | 12/2022 |
| A.23 | Budovanie spôsobilostí na audit kybernetickej bezpečnosti | Aktualizovať certifikačnú schému pre certifikáciu audítorov kybernetickej bezpečnosti podľa osobitného predpisu a podľa normy STN EN ISO/IEC 17024 „Posudzovanie zhody. Všeobecné požiadavky na orgány vykonávajúce certifikáciu osôb (ISO/IEC | NBÚ | KCCKB | 12/2022 |

| | | | | | |
|---|---|---|---|---|---|
| | | 17024)“, na základe doterajších praktických skúseností. | | | |
| A.24 | Budovanie spôsobilostí v riadení kybernetickej bezpečnosti | Dosiahnuť akreditáciu pre certifikáciu manažérov kybernetickej bezpečnosti podľa osobitného predpisu a podľa normy STN EN ISO/IEC 17024 | KCCKB | SNAS | 12/2021 |
| A.25 | Zavedenie funkčných procesov riadenia rizík kybernetickej bezpečnosti | Na riadne zabezpečenie implementácie bezpečnostných opatrení podľa zákona o kybernetickej bezpečnosti, vytvoriť rámec riadenia rizík v kybernetickej bezpečnosti upotrebiteľného pre PZS, systematické a kontinuálne riadenie rizík kybernetickej bezpečnosti v jednotlivých sektoroch. | NBÚ | ÚOOÚ SR | 06/2022 |
| A.26 | Budovanie spôsobilostí na posudzovanie zhody v kybernetickej bezpečnosti | Vytvoriť certifikačné schémy na široké portfólio typov výrobkov, procesov a služieb kybernetickej bezpečnosti v zmysle Nariadenia EÚ č. 2019/881 o agentúre ENISA a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií. | NBÚ | SNAS, ÚOOÚ SR, orgány posudzova-nia zhody | 10/2025 |
| A.27 | Posudzovanie zhody v kybernetickej bezpečnosti | Certifikovať výrobky, procesy a služby kybernetickej bezpečnosti v zmysle Nariadenia EÚ č. 2019/881 o agentúre ENISA a o certifikácii kybernetickej bezpečnosti, informačných a komunikačných technológií. | Vnútroštátny certifikačný orgán | ostatné orgány posudzova-nia zhody | priebežne |
| A.28 | Podpora spôsobilostí subjektov v oblasti riadenia kontinuity činností | Vytvoriť rámec pre oblasti riadenia kontinuity činností a havarijného plánovania v kybernetickej bezpečnosti | NBÚ | | 06/2022 |
| A.29 | Vytvorenie komunity kybernetickej bezpečnosti | Efektívna spolupráca zainteresovaných strán na všetkých úrovniach riešenia kybernetickej bezpečnosti s dôrazom na mimovládne organizácie | NBÚ | Ústredné orgány, KCCKB, záujmové zväzy, združenia a asociácie | 12/2021 |

| | | | | | |
|---|---|---|---|---|---|
| | | | | v oblasti kybernetickej bezpečnosti | |
| A.30 | Návrh indexu pre oblasť kybernetickej bezpečnosti a jeho pravidelné vyhodnocovanie | Navrhnúť metodiku pravidelného merania stavu pre oblasť kybernetickej bezpečnosti a pravidelne ho vyhodnocovať s cieľom získať vždy reálny a aktuálny prehľad a informáciu o trendoch o stave kybernetickej bezpečnosti na národnej úrovni | NBÚ | Ústredné orgány, KCCKB | 02/2022 |
| A.31 | Zavedenie systému včasného varovania v kybernetickom priestore | Zaviesť do prevádzky technicky a procesne funkčný systém včasného varovania voči kybernetickým hrozbám na podporu bezpečnosti, obranyschopnosti a obrany kybernetického priestoru Slovenskej republiky | VS, NBÚ, SIS | MIRRI SR | 12/2025 |

## 2. Efektívne odhaľovanie a objasňovanie počítačovej kriminality

| Kód úlohy | Úloha | Popis úlohy | Zodpovedný subjekt | Súčinný subjekt | Časový horizont realizácie |
|---|---|---|---|---|---|
| B.1 | Zefektívnenie NES | Zanalyzovať možnosti zefektívnenia fungovania Národnej expertnej skupiny na riešenie problematiky v oblasti počítačovej kriminality (NES) a následne implementovať vzniknuté odporúčania tak, aby sa zlepšila výmena relevantných informácií a riešenie identifikovaných problémov. | MV SR | členovia Národnej expertnej skupiny pre počítačovú kriminalitu | 12/2021 |
| B.2 | Rozvoj spolupráce s vybranými vysokými školami v oblasti počítačovej kriminality | Vytvoriť a implementovať program spolupráce s vybranými vysokými školami v oblasti počítačovej kriminality za účelom výchovy nových odborníkov a šírenia povedomia o tomto druhu kriminality tak, aby každý absolvent mal minimálny základ v tejto | MV SR | NBÚ, GP SR, MŠVVaŠ SR, ÚOOÚ SR, vybrané vysoké školy | 07/2022 |

| | | | | | |
|---|---|---|---|---|---|
| | | problematike (aktivity ako pravidelné prednášky, vedenie špecializovaných predmetov, vedenie záverečných prác, prepojenie teórie s praxou a podobne). | | | |
| B.3 | Príprava vzdelávacích programov pre justičné orgány | Vytvoriť koncept systematického špecializovaného a interdisciplinárneho vzdelávania právnych čakateľov prokuratúry a prokurátorov (vrátane členov Vnútroštátnej siete prokurátorov na boj proti počítačovej kriminalite), sudcov, vyšších súdnych úradníkov v oblasti počítačovej kriminality so zameraním sa najmä na vnútroštátne a cezhraničné zabezpečovanie elektronických dôkazov, digitálnych stôp a podobne. | Justičná akadémia | MS SR, GP SR, MV SR, NBÚ | 01/2022 |
| B.4 | Systematické vzdelávanie justičných orgánov | Na základe vytvoreného konceptu systematicky vzdelávať právnych čakateľov prokuratúry a prokurátorov (vrátane členov Vnútroštátnej siete prokurátorov na boj proti počítačovej kriminalite), sudcov, vyšších súdnych úradníkov v oblasti počítačovej kriminality s minimálnou frekvenciou kurzov 2x ročne/kurz | Justičná akadémia | MS SR, GP SR, MV SR, NBÚ | 2x ročne |
| B.5 | Koncept vzdelávania policajtov | Vytvoriť koncept špecialistov pre počítačovú kriminalitu na úrovni základných útvarov, vyšetrovania a kriminalisticko-expertíznych činností a ich pravidelného vzdelávania | MV SR | | 12/2021 |
| B.6 | Implementácia konceptu vzdelávania policajtov | Pravidelne uskutočňovať základné a rozšírené kurzy boja proti počítačovej kriminalite podľa konceptu vzdelávania špecialistov pre počítačovú kriminalitu so zameraním sa na špecifiká zaisťovania stôp, prípravného konania a operatívnych postupov, s frekvenciou minimálne 3x ročne/kurz | MV SR | | 3x ročne |
| B.7 | Prehodnocovanie a prispôsobovanie kurzov počítačovej kriminality | Pravidelne prehodnocovať kurzy boja proti počítačovej kriminalite pre príslušníkov PZ a prispôsobovanie osnov podľa aktuálnych potrieb, | MV SR | | najmenej 1x ročne |

| | | | | | |
|---|---|---|---|---|---|
| | | ktoré vzniknú na základe analýzy bezpečnostného prostredia | | | |
| B.8 | Podanie žiadosti o zápis znaleckého ústavu | Podať žiadosť o zápis KCCKB do zoznamu znalcov, tlmočníkov a prekladateľov, oddielu na zápis znalcov, časti na zápis znalcov, ktorí vykonávajú činnosť ako znalecké ústavy, do odboru pokrývajúceho oblasť kybernetickej bezpečnosti | KCCKB | | 12/2022 |
| B.9 | Koncept vzdelávania znalcov | Vytvoriť koncept vzdelávania znalcov v oblasti počítačovej kriminality so zameraním sa najmä na analýzu a vyhodnocovanie digitálnych stôp | KCCKB | znalecké ústavy | 06/2022 |
| B.10 | Implementácia konceptu vzdelávania znalcov | Na základe vytvoreného konceptu systematicky vzdelávať znalcov v oblasti počítačovej kriminality s frekvenciou minimálne 3x ročne/kurz | KCCKB | znalecké ústavy | 3x ročne |
| B.11 | Zefektívnenie zabezpečovania užívateľských údajov pre trestné konanie | Vykonať analýzu efektívnosti získavania užívateľských údajov v trestnom konaní a aplikovať získané poznatky z analýzy do právneho poriadku | MS SR | GP SR, MDaV SR | 12/2022 |
| B.12 | Odstránenie legislatívnych prekážok | Zanalyzovať možné riešenia efektívneho vyšetrovania vrátane moderných procesných inštitútov trestných činov súvisiacich s počítačovou kriminalitou | MV SR | GP SR, MS SR, SIS, VS | 12/2021 |
| B.13 | Implementácia zistení | Implementovať riešenia efektívneho vyšetrovania trestných činov, vrátane moderných procesných inštitútov súvisiacich počítačovou kriminalitou do legislatívy na základe predchádzajúcej analýzy | MS SR | GP SR, MV SR | 12/2022 |
| B.14 | Legislatívna úprava v kontexte pripravovanej legislatívy EÚ | Pripraviť legislatívne a praktické predpoklady pre realizáciu novej právnej úpravy cezhraničného zabezpečovania elektronických dôkazov a ich technická implementácia | MS SR<br>MDaV SR | GP SR | 2023 |
| B.15 | Analýza súčasného stavu tvorby a vyhodnocovania štatistických ukazovateľov trestnej činnosti súvisiacich s počítačovou kriminalitou | Zanalyzovať a vyhodnotiť súčasný stav štatistického vyhodnocovania so zameraním sa na nedostatky a rozdiely pri vykazovaní jednotlivými zainteresovanými subjektmi, ako aj na nedostatky v | Štatistický úrad, NBÚ | MV SR, GP SR, MS SR | 07/2023 |

| | | | | | |
|---|---|---|---|---|---|
| | | štatistických ukazovateľoch a následné vytvorenie metodiky pre lepšie štatistické vyhodnocovanie | | | |
| B.16 | Implementácia metodiky pre lepšie štatistické vyhodnocovanie | Implementovať metodiku pre lepšie štatistické vyhodnocovanie počítačovej kriminality pre jednotlivé zainteresované subjekty | MV SR<br>GP SR<br>MS SR | | 07/2024 |
| B.17 | Zefektívnenie zaisťovania elektronických stôp | Vytvoriť podmienky a postupy v rámci expertíznej činnosti tak, že pri zabezpečovaní elektronických stôp musí byť prítomný kriminalistický technik kvalifikovaný v oblasti počítačovej kriminality alebo iná kompetentná osoba za účelom koordinácie a výkonu ďalších činností (napr. prizvanie znalca a podobne) | MV SR | GP SR | 01/2022 |
| B.18 | Rozvoj metodickej činnosti | Pravidelne analyzovať, prehodnocovať a rozvíjať metodickú činnosť v oblasti počítačovej kriminality so zameraním sa na vydávanie metodických pomôcok a usmernení | MV SR | NBÚ, GP SR | Priebežne |

# 3. Odolný súkromný sektor

| Kód úlohy | Úloha | Popis úlohy | Zodpovedný subjekt | Súčinný subjekt | Časový horizont realizácie |
|---|---|---|---|---|---|
| C.1 | Tréningy a cvičenia pre súkromný sektor | Organizovať a podporovať praktické cvičenia súvisiace so zabezpečením pripravenosti zamestnancov prevádzkovateľov základných služieb v oblasti reakcie na kybernetické bezpečnostné incidenty, plánovania kontinuity činností, riadenia rizík a riadenia kybernetickej bezpečnosti. | NBÚ | PZS | 3x ročne |
| C.2 | Vytvorenie inkubátorov kybernetickej bezpečnosti | Pripraviť právny rámec pre vytvorenie inkubátorov kybernetickej bezpečnosti pre malé firmy (startupy) a prepojiť tak vedu a výskum so súkromným | MH SR | MF SR, MIRRI SR, NBÚ | 01/2023 |

| | | | | | |
|---|---|---|---|---|---|
| | | sektorom a podporovať vznik inovácií v oblasti kybernetickej bezpečnosti | | | |
| C.3 | Dotačné schémy pre prevádzkovateľov základných služieb | Vytvoriť a udržiavať dotačné schémy pre prevádzkovateľov základných služieb zameraných na budovanie spôsobilostí v oblasti kybernetickej bezpečnosti | MH SR | MF SR, MIRRI SR | 01/2023 |
| C.4 | Harmonizácia pravidiel pre hlásenie incidentov | Vytvoriť model hlásenia incidentov tak, aby povinný subjekt hlásil incidenty prostredníctvom jedného miesta, aj keď sa týkajú rozličných povinností (napr. zo zákona o kybernetickej bezpečnosti, nariadenia GDPR, zákona o ochrane osobných údajov a pod.) spolu s vytvorením jednotného katalógu typov incidentov | NBÚ | ÚOOÚ SR, NBS, ÚPREKaPS | 01/2022 |
| C.5 | Testovanie odolnosti infraštruktúry súkromného sektora | Vybudovať právny rámec a spôsobilosti na vykonávanie kontrolovaných testov voči prevádzkovateľom základných služieb a poskytovateľom digitálnych služieb za účelom zistenia ich odolnosti a stavu vyspelosti v oblasti kybernetickej bezpečnosti. | NBÚ | PZS | 06/2023 |
| C.6 | Vytvorenie platformy výmeny informácií v oblasti kybernetickej bezpečnosti | Vytvoriť platformu pre efektívnu spoluprácu, zdieľanie informácii a odbornú diskusiu verejného sektora so súkromným sektorom v oblasti kybernetickej bezpečnosti | NBÚ | PZS | 12/2021 |

# 4. Kybernetická bezpečnosť ako základná súčasť verejnej správy

| Kód úlohy | Úloha | Popis úlohy | Zodpovedný subjekt | Súčinný subjekt | Časový horizont realizácie |
|---|---|---|---|---|---|
| D.1 | Zjednotenie postupov a bezpečnostných opatrení a kontinuálne presadzovanie ich implementácie vo verejnej správe | Vypracovať jednotný metodický rámec pre implementáciu opatrení kybernetickej bezpečnosti podľa vyhlášky č. 179/2020 Z. z. Úradu podpredsedu vlády SR pre investície a informatizáciu, ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy. | MIRRI SR | | 03/2022 |
| D.2 | | Vytvoriť šablóny a vzory dokumentácie bezpečnosti informačných technológií verejnej správy, návodov, školiacich materiálov a ukážok v rozsahu definovanom v §1 ods. (4) vyhlášky č. 179/2020 Z. z. Úradu podpredsedu vlády SR pre investície a informatizáciu, ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy. | MIRRI SR | | 03/2022 |
| D.3 | | Vytvoriť proces a príslušné nástroje na samohodnotenie úrovne implementovaných bezpečnostných opatrení kybernetickej bezpečnosti podľa vyhlášky č. 179/2020 Z. z. Úradu podpredsedu vlády SR pre investície a informatizáciu, ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy. | MIRRI SR | | 06/2023 |
| D.4 | | Vytvoriť metodiku riadenia kybernetickej bezpečnosti vo vzťahu s tretími stranami v oblasti zaistenia bezpečnosti pri dodávateľských službách. | MIRRI SR | | 03/2022 |

| | | | | | |
|---|---|---|---|---|---|
| D.5 | Zabezpečovanie prevencie a riešenia závažných bezpečnostných incidentov vo verejnej správe prostredníctvom jednotky CSIRT.SK | Vytvoriť a zaviesť rámec pre pravidelné hodnotenie zraniteľností a penetračné testovanie informačných systémov verejnej správy majúcich rozhranie s internetom. | MIRRI SR | | 06/2023 |
| D.6 | | Nasadiť nástroje na rozpoznávanie, monitorovanie a riadenie bezpečnostných incidentov v prostredí verejnej správy. | MIRRI SR | | 03/2025 |
| D.7 | | Vytvoriť odbornú metodiku pre vznik odborných bezpečnostných pracovísk (nazývaných CSIRT) v prostredí verejnej správy. | MIRRI SR | | 12/2023 |
| D.8 | | Vytvoriť centrálny katalóg hrozieb pre verejnú správu. | MIRRI SR | | 12/2022 |
| D.9 | | Vytvoriť postup pre implementáciu bezpečnostných záplat na zraniteľné informačné systémy a aplikácie v prostredí verejnej správy. | MIRRI SR | | 03/2023 |
| D.10 | Zabezpečenie adekvátnych odborných kapacít verejnej správy | Určiť schému nevyhnutných počtov obsadenia odbornými pozíciami v jednotlivých orgánoch verejnej správy a spôsobu ich naplnenia. | MIRRI SR | | 03/2022 |
| D.11 | | Definovať pracovné pozície v oblasti kybernetickej bezpečnosti vo verejnej správe a znalostné požiadavky pre jednotlivé pozície. | MIRRI SR | NBÚ Akademický sektor, tretí sektor, zástupcovia miest a obcí | 11/2022 |

# 5. Silné partnerstvá

| Kód úlohy | Úloha | Popis úlohy | Zodpovedný subjekt | Súčinný subjekt | Časový horizont realizácie |
|---|---|---|---|---|---|
| E.1 | Aktívna participácia na medzinárodnej diskusii v oblastiach kybernetickej bezpečnosti a kybernetickej diplomacie a následná implementácia dohodnutých záväzkov | Aktívne sa zapájať do tvorby a implementácie politík a nástrojov EÚ v oblasti kybernetickej bezpečnosti. Aktívne pôsobiť a presadzovať záujmy SR v rámci Horizontálnej pracovnej skupiny pre kybernetické záležitosti. | NBÚ | | priebežne |
| E.2 | | Aktívne sa podieľať na implementácii Stratégie kybernetickej bezpečnosti EÚ. | NBÚ | MZVEZ SR | priebežne |
| E.3 | | Posilniť a rozšíriť kybernetický dialóg s tretími štátmi, medzinárodnými organizáciami (vrátane regionálnych zoskupení) aj prostredníctvom neformálnej siete kybernetickej diplomacie EÚ. | MZVEZ SR | NBÚ | priebežne |
| E.4 | | Spolupracovať so spojencami pri implementácii politík a posilňovaní nástrojov NATO v oblasti kybernetickej obrany v kontexte kolektívnej obrany. | NBÚ, MO SR | MZVEZ SR | priebežne |
| E.5 | | Plniť záväzok č. 11 v rámci Stálej štruktúrovanej spolupráce Európskej únie (PESCO) a zabezpečiť väčšie úsilie pri spolupráci v oblasti kybernetickej obrany, ako sú výmena informácií, odborná príprava a operačná podpora. | MO SR | | priebežne |
| E.6 | Aktívne pôsobenie v medzinárodnom prostredí zamerané na presadenie noriem zodpovedného správania sa v kybernetickom priestore | Na pôde OSN sa zasadzovať za pokračovanie úsilia zameraného na posilnenie noriem, princípov a pravidiel používania IKT s cieľom zaviazať štáty k zodpovednému správaniu v kybernetickom priestore, uplatňovať medzinárodné právo a budovať dôveru s cieľom prevencie nestability a posilňovania bezpečnosti. | MZVEZ SR | NBÚ | priebežne |

| | | | | | |
|---|---|---|---|---|---|
| E.7 | | Aktívne sa podieľať na tvorbe a implementácii kybernetických opatrení pre budovanie dôvery medzi štátmi v kybernetickom priestore (CBMs), prípadne ďalších iniciatív, v súlade s Bezpečnostnou stratégiou SR a Národnou stratégiou kybernetickej bezpečnosti. | NBÚ | MZVEZ SR | priebežne |
| E.8 | | V rámci členstva v medzinárodných organizáciách (RE, EÚ, OSN, OECD) presadzovať riešenia, ktoré prispejú k efektívnejšiemu stíhaniu počítačovej kriminality pri zachovaní základných požiadaviek na ochranu základných práv a slobôd. | MS SR | NBÚ, MZVEZ SR | priebežne |
| E.9 | Nadväzovať a posilňovať bilaterálnu spoluprácu SR v oblasti kybernetickej bezpečnosti. | Vytvárať a posilňovať partnerskú spoluprácu s vybranými štátmi v rámci kybernetickej bezpečnosti zameranú na rozširovanie spolupráce špecializovaných inštitúcií, výmenu skúseností a najlepších praktík ako aj posilňovanie národných kapacít a expertízy v oblasti kybernetickej bezpečnosti. Zamerať sa na rozvoj strategickej spolupráce v oblasti kybernetickej bezpečnosti s krajinami s najrozvinutejšou infraštruktúrou, inštitucionálnym a expertným zázemím, poznatkami alebo reálnymi skúsenosťami v oblasti kybernetickej bezpečnosti v rámci EU (najmä AT, DE, FR, NL, EE, LV, BE, IE, FI, a EE), a mimo EU (najmä US, UK, CA, IL, JP, AU, NZ, MY, ID, KR, TW, TH, PH, AE, KW, QT, OM) | NBÚ | MZVEZ SR | priebežne |
| E.10 | | Spolupracovať s partnerskými odbornými organizáciami (Trusted Introducer, FIRST) pri budovaní kapacít SR v oblasti kybernetickej bezpečnosti a zdieľať expertízu v oblasti kybernetickej bezpečnosti od členov týchto organizácií. | NBÚ | | priebežne |
| E.11 | Posilniť systémové pokrývanie agendy kybernetickej bezpečnosti | V rámci existujúcich kapacít rozšíriť zameranie činnosti zastupiteľských úradov vo vybraných | MZVEZ SR | NBÚ | priebežne |

| | | | | | |
|---|---|---|---|---|---|
| | a diplomacie na vybraných zastupiteľstvách SR v zahraničí a zo Slovenska. | krajinách o problematiku kybernetickej bezpečnosti a diplomacie, vrátane rozširovania stykovej a spravodajskej činnosti v tejto oblasti. | | | |
| E.12 | | Pokračovať v rozvoji medzinárodnej spolupráce v agende kybernetickej bezpečnosti na vybraných zastupiteľských úradoch a z centra prostredníctvom pracovníkov NBÚ v pozícii kyber atašé a dosiahnuť pokrytie najmenej EÚ, Spojeného kráľovstva, Severnej Ameriky a Ázie. | NBÚ | MZVEZ SR | 6/2022 |
| E.13 | Podporovať zapájanie slovenských podnikov, mimovládnych organizácií, či akademickej sféry do medzinárodných aktivít a iniciatív v oblasti kybernetickej bezpečnosti. | Aktívne podporovať a vyhľadávať príležitosti pre zapájanie slovenských podnikov, mimovládnych organizácií a akademického sektora do medzinárodnej spolupráce v oblasti kybernetickej bezpečnosti, vrátane zdieľania ich expertízy a nadväzovania obchodnej spolupráce. | MZVEZ, NBÚ | KCCKB | priebežne |
| E.14 | SK-ISAC | Pripraviť a implementovať model skupín pre spoluprácu v oblasti kybernetickej bezpečnosti na sektorovej úrovni (model ISAC). | NBÚ | PZS | 12/2021 |
| E.15 | Národná CSIRT sieť | Zriadiť národnú CSIRT sieť, ktorá bude združovať CSIRT jednotky z verejného, súkromného a akademického sektora | NBÚ | MIRRI SR | 01/2022 |
| E.16 | Platforma na spoluprácu | Vytvoriť platformu na úzku spoluprácu s Centrom pre kybernetickú obranu, Národným centrom kybernetickej bezpečnosti SK-CERT a Centrom pre kybernetické spravodajstvo | NBÚ | VS, SIS | 12/2021 |
| E.17 | Spolupráca v oblasti kybernetickej obrany | Posilňovať spoluprácu rezortu obrany s príslušnými štátnymi inštitúciami, súkromným sektorom a akademickou obcou na národnej aj medzinárodnej úrovni | MO SR | | Priebežne |
| E.18 | Kolektívna obrana | Urýchľovať implementáciu medzinárodných záväzkov SR v rámci kolektívnej obrany | MO SR | NBÚ | Priebežne |
| E.19 | Pôsobenie v medzinárodnom prostredí zamerané na | Pokračovať v rozvoji medzinárodnej spolupráce v agende kybernetickej bezpečnosti v expertných | ÚJD SR | MZVEZ SR, NBÚ | Priebežne |

| | | | | | |
|---|---|---|---|---|---|
| | optimalizáciu noriem prijatých na pôde Medzinárodnej agentúry pre atómovú energiu (MAAE) pre zodpovedné správanie sa v kybernetickom priestore jadrových zariadení | skupinách MAAE a prostredníctvom pracovníkov Úradu jadrového dozoru Slovenskej republiky (ÚJD SR) | | | |

# 6. Vzdelaní odborníci a vzdelaná verejnosť

| Kód úlohy | Úloha | Popis úlohy | Zodpovedný subjekt | Súčinný subjekt | Časový horizont realizácie |
|---|---|---|---|---|---|
| F.1 | Východiská vzdelávania v oblasti kybernetickej bezpečnosti | Vypracovať všeobecne zrozumiteľný referenčný rámec a stupne hodnotenia kompetencií v oblasti kybernetickej bezpečnosti ako súčasť digitálnych kompetencií pre účely celoživotného vzdelávania na národnej úrovni. | MŠVVaŠ SR | NBÚ, tretí sektor | 12/2021 |
| F.2 | | Zadefinovať pojem bezpečnostného povedomia vo vzdelávaní a požiadaviek na minimálne bezpečnostné návyky pri používaní IKT pre žiakov, odstupňovaný podľa veku žiakov zapracovaný do stratégie rozvoja digitálnych zručností v regionálnom školstve počnúc materskými školami a na všetkých stupňoch vysokoškolského vzdelávania. | MŠVVaŠ SR | NBÚ, tretí sektor | 03/2022 |

| | | | | | |
|---|---|---|---|---|---|
| F.3 | | Dopracovať aktuálne a vznikajúce zamestnania zaoberajúce sa kybernetickou bezpečnosťou do registra zamestnaní vrátane ich kompetenčných a kvalifikačných úrovní v rámci Národnej sústavy povolaní v súlade s Národným kvalifikačných rámcom SR a Národnou sústavou kvalifikácií (odborné vedomosti, odborné zručnosti, všeobecné spôsobilosti) | MŠVVaŠ SR | MPSVaR SR, KCCKB, Aliancia sektorových rád, tretí sektor | 03/2022 |
| F.4 | | Dopracovať profesijné štandardy pre jednotlivé kategórie a podkategórie pedagogických zamestnancov a odborných zamestnancov škôl a školských zariadení o špecifiká z oblasti kybernetickej bezpečnosti vo výchove a vzdelávaní. | MŠVVaŠ SR | NBÚ, tretí sektor | 05/2022 |
| F.5 | | Dopracovať profesijné štandardy pre jednotlivé kategórie a podkategórie pedagogických zamestnancov a odborných zamestnancov škôl a školských zariadení o špecifiká z oblasti ochrany mladých ľudí pred ujmou z nesprávneho používania IKT a internetu. | MŠVVaŠ SR | NBÚ, tretí sektor | 05/2022 |
| F.6 | | Vypracovať jednotnú metriku a vytvoriť dostupný testovací nástroj pre meranie a atestáciu stupňov kompetencií v oblasti kybernetickej bezpečnosti ako súčasť digitálnych kompetencií vo formálnom vzdelávaní i vzdelávaní dospelých. | MŠVVaŠ SR | NBÚ, MPSVaR SR, tretí sektor | 6/2022 |

| | | | | | |
|---|---|---|---|---|---|
| F.7 | Budovanie základného povedomia a vzdelávanie v kybernetickej bezpečnosti v regionálnom školstve | Zrealizovať meranie úrovne kompetencií riaditeľov, pedagogických i nepedagogických pracovníkov a žiakov škôl v regionálnom školstve pre získanie informácie o súčasnom stave, potrebe nápravy nedostatkov v povedomí o kybernetickej bezpečnosti a súvisiacich digitálnych zručnostiach a pre ich medziročné zlepšovanie. | MŠVVaŠ SR | zriaďovatelia škôl, NBÚ, tretí sektor | 12/2021 |
| F.8 | | Zrealizovať meranie úrovne kompetencií pedagógov a študentov vysokých škôl pre získanie informácie o súčasnom stave, potrebe nápravy nedostatkov v povedomí o kybernetickej bezpečnosti a súvisiacich digitálnych zručnostiach a pre ich medziročné zlepšovanie. | MŠVVaŠ SR | zriaďovatelia škôl, NBÚ, tretí sektor | 12/2021 |
| F.9 | | Pravidelne na národnej úrovni opakovať meranie úrovne kompetencií (testovanie) riaditeľov, pedagogických i nepedagogických pracovníkov a žiakov škôl v regionálnom školstve a pedagógov a študentov vysokých škôl pre získanie informácie o súčasnom stave, potrebe nápravy nedostatkov v povedomí o kybernetickej bezpečnosti a súvisiacich digitálnych zručnostiach a pre ich medziročné zlepšovanie. | MŠVVaŠ SR | zriaďovatelia škôl, NBÚ, | každoročne od 01/2022 |
| F.10 | | Navrhnúť metodiku posúdenia rizík v súvislosti s interakciou detí a mládeže s IKT a internetom, v závislosti na veku dieťaťa. | MŠVVaŠ SR | NBÚ, MV SR, zriaďovatelia škôl | 03/2022 |
| F.11 | | Udržiavať prehľad o rizikách v súvislosti s interakciou detí a mládeže s IKT a internetom, v závislosti na veku dieťaťa. | MŠVVaŠ SR | NBÚ, MV SR, zriaďovatelia škôl | každoročne od 05/2022 |

| | | | | | |
|---|---|---|---|---|---|
| F.12 | | Vytvoriť jednotné obsahové osnovy minimálnych požiadaviek pre porozumenie hrozieb vyplývajúcich z používania digitálnych technológií prierezovo pre jednotlivé ročníky ZŠ a SŠ s dôrazom na prispôsobenie formy, obsahu a metodiky podľa veku. | MŠVVaŠ SR | NBÚ, MV SR | 02/2023 |
| F.13 | | Posilniť výchovno-vzdelávací proces a pripravovanú kurikulárnu reformu v zameraní na schopnosť logického myslenia, kritického myslenia, etiky a nevyhnutných digitálnych zručností v oblasti kybernetickej bezpečnosti (medzipredmetový dosah kybernetickej bezpečnosti). | MŠVVaŠ SR | NBÚ, tretí sektor | priebežne |
| F.14 | | Podporovať využívanie vybraných bezpečných nástrojov dištančného vzdelávania a spolupráce všetkých žiakov a učiteľov (na škole i z domáceho prostredia), spolu s odporúčaním a koordináciou ich zjednoteného, odborného a bezpečného využívania na lokálnej a regionálnej úrovni. | MŠVVaŠ SR | zriaďovatelia škôl, mestá a samosprávne kraje | priebežne |
| F.15 | | Stanoviť normatívy pre zaistenie bezpečnosti internetového pripojenia v škole, zaistiť maximálnu bezpečnosť využívania koncových IKT zariadení v škole a vo výchovno-vzdelávacom procese. | MŠVVaŠ SR | zriaďovatelia škôl, obce a samosprávne kraje | 06/2024 |
| F.16 | | Pre žiakov zo sociálne znevýhodneného prostredia zabezpečiť dostupnosť, podporu a dohľad nad využívaním bezpečného internetu mimo výchovno-vzdelávacieho procesu v škole spôsobom primeraným a prispôsobeným lokálnym možnostiam (internet v domácom prostredí, alebo v komunitnom centre, alebo iným spôsobom s podporou pedagogických asistentov a podobne) | MŠVVaŠ SR | zriaďovatelia škôl, obce a samosprávne kraje | 06/2024 |

| | | | | | |
|---|---|---|---|---|---|
| F.17 | | Rozšíriť vzdelávací obsah a didaktické pomôcky škôl o prvky hier a súťaživosti pre vytvorenie a udržanie záujmu žiakov o problematiku kybernetickej bezpečnosti. | MŠVVaŠ SR | | 07/2023 |
| F.18 | | Legislatívne vymedziť a na každej škole podporovať školského IT administrátora s technickou kvalifikáciou a dostatočnými kompetenciami aj v oblasti kybernetickej bezpečnosti | MŠVVaŠ SR | zriaďovatelia škôl, mestá a samosprávne kraje | 10/2023 |
| F.19 | | Legislatívne vymedziť a na každej škole podporovať školského koordinátora digitálnej transformácie vzdelávania (digitálneho koordinátora) s pedagogickou kvalifikáciou a dostatočnými kompetenciami pre vzdelávanie v oblasti kybernetickej bezpečnosti | MŠVVaŠ SR | zriaďovatelia škôl, mestá a samosprávne kraje, tretí sektor | 10/2023 |
| F.20 | | Zabezpečiť pedagogickým i nepedagogickým pracovníkom škôl a inštruktorom odborného vzdelávania a prípravy dostatočné inovačné a aktualizačné resp. celoživotné vzdelávanie v oblasti kybernetickej bezpečnosti a v oblasti rýchlo sa rozvíjajúcich technológií a ich bezpečnostných dopadov | MŠVVaŠ SR | fakulty vysokých škôl vzdelávajúce učiteľov, špecialisti zo súkromného sektora | 12/2023 |
| F.21 | | Stanoviť normatívy materiálno-technického a priestorového zabezpečenia škôl všetkých typov, ich tried a žiakov IKT zariadeniami zabezpečenými v oblasti kybernetickej bezpečnosti. Vo finančnom normatíve pre školy zabezpečiť a priebežne overovať udržateľnosť IKT vybavenia špecifikovaného technickým predpisom. | MŠVVaŠ SR | zriaďovatelia škôl, mestá a samosprávne kraje, tretí sektor | 12/2024 |

| | | | | | |
|---|---|---|---|---|---|
| F.22 | | Podporiť rozšírenie prípravy nových pedagógov a zaviesť kontinuálne vzdelávanie aktuálnych pedagógov o oblasť kybernetickej bezpečnosti vo všetkých vzdelávacích oblastiach, primárne v oblasti práce s informáciami. | MŠVVaŠ SR | fakulty vysokých škôl vzdelávajúce učiteľov, špecialisti zo súkromného sektora | 12/2023 |
| F.23 | | Vypracovať prierezové metodiky pre učiteľov I. stupňa ZŠ a cvičebnice pre žiakov I. stupňa ZŠ v slovenskom, maďarskom a rómskom jazyku a iných podkladov pre učiteľov pre oblasť kybernetickej bezpečnosti a bezpečného správania sa na internete | MŠVVaŠ SR | MV SR, KCCKB, diagnosticko-poradenské centrá, tretí sektor, odborná verejnosť | 12/2022 |
| F.24 | | Zlepšovať spoluprácu medzi aktérmi, pôsobiacimi v ochrane detí v kybernetickom priestore | MPSVaR SR | MV SR, MŠVVaŠ SR, diagnosticko-poradenské centrá, tretí sektor, odborná verejnosť | priebežne |
| F.25 | | Vytvoriť grantové schémy na podporu zvyšovania bezpečnostného povedomia v oblasti kybernetickej bezpečnosti a bezpečného správania sa na internete so zameraním sa na deti a mládež | MŠVVaŠ SR | MF SR, KCCKB | 12/2022 |
| F.26 | Vzdelávanie a príprava kvalitných IT špecialistov na kybernetickú bezpečnosť | Vytvoriť koncept podpory odborného vzdelávania a v skupine odborov 25 IKT na stredných odborných školách v oblasti kybernetickej bezpečnosti | MŠVVaŠ SR | ŠIOV, stredné odborné školy a ich zriaďovatelia, RUZ | 06/2022 |

| | | | | | |
|---|---|---|---|---|---|
| F.27 | | Inovovať školské vzdelávacie programy a vytvoriť a overiť 10 vzorových školských vzdelávacích programov stredných odborných škôl so zapracovanými požiadavkami v oblasti kybernetickej bezpečnosti podľa aktuálneho vývoja a požiadaviek na trhu práce, v spolupráci so zamestnávateľmi súkromnej sféry a fakultami vysokých škôl technického zamerania | MŠVVaŠ SR | ŠIOV, stredné odborné školy a ich zriaďovatelia, RUZ, súkromný sektor, vysoké školy | 12/2022 |
| F.28 | | Vybaviť stredné školy vzdelávajúce v skupine odborov 25 IKT technológiou a laboratóriami pre podporu výuky predmetov zameraných na kybernetickú bezpečnosť | MŠVVaŠ SR | stredné odborné školy a ich zriaďovatelia | 06/2024 |
| F.29 | | Revidovať a navýšiť normatív pre udržateľnosť kvality vzdelávania v skupine odborov 25 IKT so zameraním sa na kybernetickú bezpečnosť | MŠVVaŠ SR | ŠIOV, stredné odborné školy a ich zriaďovatelia | 12/2022 |
| F.30 | | Podporiť vypracovanie dvoch nových odborov na stupni vzdelávania "Q" pre prvý stupeň terciárneho vzdelávania (ISCED B5) pomaturitného resp. špecializačného vzdelávania vrátane ich profilácie na kybernetickú bezpečnosť | MŠVVaŠ SR | ŠIOV, stredné odborné školy a ich zriaďovatelia, RUZ | 01/2023 |
| F.31 | | Aktualizovať a doplniť technologické vybavenie programu Sieťových akadémií na Slovensku pre podporu vzdelávania špecialistov na vysokých a stredných školách v oblasti kybernetickej bezpečnosti. | MŠVVaŠ SR | Vysoké školy, stredné školy, tretí sektor | 01/2024 |
| F.32 | | V rámci relevantných a existujúcich vysokoškolských študijných odborov vytvoriť a akreditovať študijné predmety v oblasti kybernetickej bezpečnosti | Fakulty relevantných vysokých škôl | Vysoké školy | 12/2021 |

| | | | | | |
|---|---|---|---|---|---|
| F.33 | | Vytvoriť a akreditovať vysokoškolské študijné odbory v oblasti kybernetickej bezpečnosti | MŠVVaŠ SR | Vysoké školy | 08/2022 |
| F.34 | | Vytvoriť a akreditovať vysokoškolský študijný program kybernetická bezpečnosť alebo rozšíriť akreditáciu už niektorého z relevantných študijných programov | MŠVVaŠ SR | Vysoké školy, zriaďovatelia Vysokých škôl | 08/2024 |
| F.35 | | Vytvoriť koncepciu vzdelávania kybernetickej bezpečnosti na všetkých typoch vysokých škôl | MŠVVaŠ SR | Vysoké školy | 12/2022 |
| F.36 | | Vytvoriť legislatívne prostredie, naviazané na potreby zamestnávateľov v oblasti zvyšovania zručností zamestnancov pre využívanie prvého stupňa terciárneho vzdelávania na stredných odborných školách v prepojení na potreby praxe a možnosti pokračovania vo vysokoškolskom vzdelávaní, prípadne externej formy štúdia zamestnanca na vysokých školách v študijných odboroch a programoch v oblasti kybernetickej bezpečnosti a podpora vzdelávania dospelých v kurzoch v oblasti kybernetickej bezpečnosti | MŠVVaŠ SR | MPSVaR, Rada zamestnáva-teľov pre OVP | 12/2022 |
| F.37 | | Posilniť popularizáciu stredoškolského i vysokoškolského štúdia technických a prírodovedných odborov (STEM) a kybernetickej bezpečnosti | MŠVVaŠ SR | | 12/2022 |
| F.38 | | Podporovať regionálne nadpodnikové centrá praxe a inovácií pre zapájanie špecialistov kybernetickej bezpečnosti zo súkromného sektora a doktorandov vysokých škôl do odborného vzdelávania a prípravy | MŠVVaŠ SR | MPSVaR SR, zamestnáva-teľské zväzy, Rada zamestnáva-teľov pre OVP, samosprávne kraje | 12/2022 |

| | | | | | |
|---|---|---|---|---|---|
| F.39 | Vzdelávanie a zvyšovanie bezpečnostného povedomia zamestnancov verejnej správy | Vytvoriť program vzdelávania a zvyšovania bezpečnostného povedomia pre pracovníkov verejnej správy v oblasti získavania odborných kompetencií a minimálnych vedomostných štandardov v oblasti kybernetickej bezpečnosti vrátane doplnkového vzdelávania špecialistov kybernetickej bezpečnosti. | MIRRI SR | Akademický sektor<br>KCCKB<br>MŠVVaŠ SR<br>SIS | 12/2022 |
| F.40 | | Vytvoriť plán financovania, prijímania, udržania, zabezpečenia a kariérneho rastu zamestnancov verejnej správy. | MIRRI SR | | 12/2022 |
| F.41 | | Zaviesť vzdelávanie manažérov kybernetickej bezpečnosti a informačnej v sektore verejnej správy. | MIRRI SR | KCCKB<br>Akademický sektor<br>Súkromný sektor | 10/2023 |
| F.42 | | Vytvoriť centrá excelentnosti pre kybernetickú bezpečnosť na vysokých školách v SR z dôvodu spolupráce pri výskume, vývoji a celoživotnom vzdelávaní v oblasti kybernetickej bezpečnosti pre zabezpečenie potrebných kapacít a zručností a vývoj nových riešení. | MŠVVaŠ SR | MIRRI SR<br>KCCKB<br>Akademický sektor<br>SAV<br>Slovenská rektorská konferencia | 03/2025 |
| F.43 | | Systémovo posilniť povedomie zamestnancov a príslušníkov rezortu obrany v oblasti kybernetickej bezpečnosti v pôsobnosti rezortu obrany | MO SR | | 12/2021 |
| F.44 | | Systémovo prehlbovať odborné vzdelávanie a zručnosti zamestnancov a príslušníkov rezortu obrany na úseku kybernetickej bezpečnosti v podmienkach rezortu obrany | MO SR | | 06/2022 |

| | | | | | |
|---|---|---|---|---|---|
| F.45 | | Vykonávať výcvik, zameraný na posilňovanie zručností zamestnancov a príslušníkov rezortu obrany v oblasti kybernetickej bezpečnosti, vrátane účasti na národných a medzinárodných cvičeniach kybernetickej obrany | MO SR | NBÚ | priebežne |
| F.46 | Zvyšovanie povedomia o možnosti ochrany detí pohybujúcich sa na internete spolu s vytvorením možnosti anonymného požiadania a psychosociálnu pomoc | Vytvoriť webový portál s informáciami, zameranými na prevenciu pred ohrozením detí pri používaní IKT a internetu spolu s možnosťou včasnej pomoci a online intervencie odborníka (možnosť diskrétnej komunikácie s dieťaťom) | MV SR | MŠVVaŠ SR, MPSVaR SR, psychologicko-poradenské centrá, regionálna a obecná verejná správa, tretí sektor | 01/2023 |
| F.47 | | Vytvoriť koncept vzdelávania online terénnych pracovníkov, ktorí aktívne vyhľadávajú obete kyberšikany, vykonávajú včasnú intervenciu a sú k dispozícii pre dôvernú komunikáciu s ohrozeným dieťaťom | MV SR | MŠVVaŠ SR, MPSVaR SR, psychologicko-poradenské centrá, regionálna a obecná verejná správa, tretí sektor | 01/2023 |
| F.48 | Vzdelávanie seniorov a ohrozených skupín | Iniciovať a podporiť vzdelávanie dospelých a zvyšovanie povedomia o kybernetickej bezpečnosti znevýhodnených skupín, najmä seniorov, zamestnancov nad 55 rokov a osôb v domácnosti | MV SR | MŠVVaŠ SR, regionálne a obecné samosprávy, ZMOS | 06/2022 |

| | | | | | |
|---|---|---|---|---|---|
| F.49 | Koncept zvyšovania bezpečnostného povedomia | Vytvoriť plán šírenia bezpečnostného povedomia v oblasti kybernetickej bezpečnosti | NBÚ | | 12/2021 |
| F.50 | Kampane zvyšovania povedomia | Organizovať a viesť kampane na zvyšovanie povedomia v oblasti kybernetickej bezpečnosti | NBÚ | sektorové ústredné orgány | priebežne |
| F.51 | E-learningový systém pre podporu budovania bezpečnostného povedomia a vzdelávania v oblasti kybernetickej bezpečnosti | Vytvoriť a zaviesť e-learningový systém pre podporu budovania bezpečnostného povedomia a vzdelávania v oblasti kybernetickej bezpečnosti. Systém bude zohľadňovať hierachiu zainteresovaných rolí a špecifiká sektorov. | NBÚ | KCCKB | 12/2023 |
| F.52 | Projekty a programy v oblasti vzdelávania a šírenia bezpečnostného a situačného povedomia | Podporovať a zaviesť nástroje dištančného vzdelávania v oblasti kybernetickej bezpečnosti za účelom šírenia bezpečnostného a situačného povedomia | NBÚ | KCCKB, MŠVVaŠ SR, Vysoké školy | 12/2023 |
| F.53 | | Vytvoriť projekty na tvorbu open source programov v danej oblasti vzdelávania a šírenia situačného povedomia | KCCKB | NBÚ | 06/2022 |
| F.54 | Výcvik a cvičenia v oblasti kybernetickej bezpečnosti | Vytvoriť centrum na organizovanie cvičení, výcviku a vzdelávacích aktivít v oblasti kybernetickej bezpečnosti | NBÚ | SIS, MIRRI SR | 12/2023 |
| F.55 | Vzdelávanie diplomatov | Zaviesť problematiku kybernetickej bezpečnosti a diplomacie ako integrálnu súčasť atestačného vzdelávania a odbornej prípravy pracovníkov a zamestnancov ústredných orgánov štátnej správy, vysielaných do zahraničia. | MZVEZ SR | NBÚ, MO SR | priebežne |

# 7. Rozvoj výskumu a vývoja v oblasti kybernetickej bezpečnosti

| Kód úlohy | Úloha | Popis úlohy | Zodpovedný subjekt | Súčinný subjekt | Časový horizont realizácie |
|---|---|---|---|---|---|
| G.1 | Budovanie výskumnej / experimentálnej siete | Vybudovať výskumnú / experimentálnu sieť na zdieľanie bezpečnostných udalostí a iných údajov získaných bezpečnostnými dohľadovými systémami medzi rôznymi typmi výskumných organizácií (univerzity, SAV, súkromný sektor, štát). Súčasťou aktivity je aj vytvorenie postupov a metodík pre návrh, implementáciu a prevádzku dohľadových systémov | CVTI | NBÚ, MIRRI SR Vysoké školy, SAV, a súkromný sektor | 01/2023 |
| G.2 | Budovanie univerzitných SOC a CSIRT tímov | Vybudovať bezpečnostné dohľadové centrá (SOC) a tímy na riešenie počítačových bezpečnostných incidentov (CSIRT) v rámci vysokých škôl a SAV | SAV, vysoké školy | | 06/2023 |
| G.3 | Budovať odborné kapacity bezpečnostných tímov vrátane ich odborného vzdelávania | Vytvoriť odborné pozície na vysokých školách za účelom prevádzky bezpečnostných systémov pre zber údajov a riešenie bezpečnostných incidentov. | Vysoké školy | SAV, súkromný sektor | priebežne |
| G.4 | Výskum v oblasti kybernetickej bezpečnosti pomocou metód umelej inteligencie | Vytvoriť výskumné pozície na vybraných vysokých školách a SAV za účelom realizácie výskumu a vývoja v konkrétnych oblastiach kybernetickej bezpečnosti. | SAV, Vybrané vysoké školy | súkromný sektor | priebežne |
| G.5 | Vytvorenie konzorcia pre výskum v oblasti kybernetickej bezpečnosti | Vytvoriť konzorcium pre výskum v oblasti kybernetickej bezpečnosti za účelom prepojenia vysokých škôl, SAV, súkromného a verejného sektora a koordináciu výskumných aktivít v oblasti kybernetickej bezpečnosti | NBÚ | Vysoké školy, SAV, KCCKB, SIS, MIRRI SR | 12/2021 |
| G.6 | Zmapovať súčasný stav vedy a výskumu v oblasti kybernetickej bezpečnosti na Slovensku | Identifikovať existujúce výskumné aktivity a projekty s cieľom prepojiť a integrovať výskum a zabezpečiť, že sa nebude robiť duplicitný výskum, ale tímy sa budú integrovať a svoju prácu budú navzájom koordinovať. | CVTI | NBÚ | 01/2022 |

| | | | | | |
|---|---|---|---|---|---|
| G.7 | Definovanie tém výskumu v oblasti kybernetickej bezpečnosti | Vytvoriť úvodný zoznam výskumných tém v oblasti kybernetickej bezpečnosti a ich pravidelná aktualizácia (minimálne raz ročne). | Konzorcium | | 02/2022 a následne raz ročne |
| G.8 | Výskumné projekty v oblasti kybernetickej bezpečnosti | Vypísať projektové výzvy za účasti členov Konzorcia a súkromného sektora s riešením úloh v súlade s definovanými témami kybernetickej bezpečnosti | MIRRI SR | Konzorcium, MŠVVaŠ SR, KCCKB | 01/2023 |
| G.9 | Zdieľanie dát pre výskumné účely | Vytvoriť systém a podmienky pre zdieľanie dát pre výskumné účely za účelom trénovania a testovania neurónových sietí, pre metódy strojového učenia a iné výskumné účely | Konzorcium | Vysoké školy, SAV, NBÚ, MIRRI SR, súkromný sektor | 06/2022 |
| G.10 | Prepojenie na medzinárodné konzorciá v oblasti výskumu kybernetickej bezpečnosti | Vytvoriť funkčné prepojenie s poprednými výskumnými tímami minimálne v krajinách - Česko, Poľsko, Maďarsko, Rakúsko a zapojenie sa do medzinárodných iniciatív | MŠVVaŠ SR | Vysoké školy, SAV, sukromný sektor | 12/2023 |
| G.11 | Podpora projektov v kybernetickej bezpečnosti v rámci plnenia úlohy národného koordinačného centra ECCC | Realizovať a podporiť implementácie projektov kybernetickej bezpečnosti z európskych štrukturálnych a investičných fondov a iných finančných nástrojov Európskej únie a zabezpečenie ich prevádzky | KCCKB | MIRRI SR | 12/2021 |
| G.12 | Publikačná činnosť v kybernetickej bezpečnosti | Podporovať publikačnú činnosť v oblasti kybernetickej bezpečnosti a kontinuálne uverejňovať odborné články a vedecké práce v tejto oblasti | KCCKB | MŠVVaŠ SR, NBÚ, Vysoké školy | priebežne |
| G.13 | Technická normalizácia v kybernetickej bezpečnosti | Podľa potrieb technickej verejnosti alebo príslušných orgánov verejnej moci podporovať prijímanie európskych noriem a medzinárodných noriem v oblasti informačnej a kybernetickej bezpečnosti do sústavy STN najmä prekladom do štátneho jazyka | KCCKB | ÚNMS SR | 06/2021 a následne priebežne |
| G.14 | Vytvorenie grantovej agentúry | Vytvoriť grantovú agentúru KCCKB a MŠVVaŠ SR za účelom tvorby a poskytovania grantových schém v oblasti výskumu a vývoja v oblasti kybernetickej bezpečnosti | KCCKB | MŠVVaŠ SR | 06/2022 |

| | | | | | |
|---|---|---|---|---|---|
| G.15 | Poskytovanie grantových schém | Poskytovať grantové schémy pre výskumné centrá na vysokých školách v oblasti kybernetickej bezpečnosti | KCCKB | MŠVVaŠ SR, Vysoké školy | priebežne |
| G.16 | | Poskytovať grantové schémy pre výskumné centrá na národnej úrovni a pre súkromné spoločnosti v oblasti kybernetickej bezpečnosti | KCCKB | MŠVVaŠ SR, súkromný sektor | priebežne |

# Zoznam skratiek

CVTI - Centrum vedecko-technických informácií
GP SR - Generálna prokuratúra
IKT – Informačné a komunikačné technológie
KCCKB - Kompetenčné a certifikačné centrum kybernetickej bezpečnosti
Konzorcium – Konzorcium, ktoré vznikne na základe úlohy G.5
MAAE - Medzinárodná agentúra pre atómovú energiu
MDaV SR - Ministerstvo dopravy a výstavby SR
MF SR - Ministerstvo financií SR
MH SR - Ministerstvo hospodárstva SR
MIRRI SR - Ministerstvo investícií, regionálneho rozvoja a informatizácie SR
MO SR - Ministerstvo obrany SR
MPSVaR SR - Ministerstvo práce, sociálnych vecí a rodiny SR
MS SR - Ministerstvo spravodlivosti SR
MŠVVaŠ SR - Ministerstvo školstva, vedy, výskumu a športu SR
MV SR - Ministerstvo vnútra SR
MZVEZ SR - Ministerstvo zahraničných vecí a európskych záležitostí SR
NBS - Národná banka Slovenska
NBÚ - Národný bezpečnostný úrad
NCKB SK-CERT – Národné centrum kybernetickej bezpečnosti SK-CERT
NES - Národná expertná skupina

OVP - Odborné vzdelávanie a príprava
PDS – Poskytovatelia digitálnych služieb
PZS - Prevádzkovatelia základných služieb
SAV - Slovenská akadémia vied
SIS - Slovenská informačná služba
SNAS - Slovenská národná akreditačná služba
ŠIOV - Štátny inštitút odborného vzdelávania
ŠS - Štátna správa
RUZ - Republiková únia zamestnávateľov
ÚJD SR - Úrad jadrového dozoru Slovenskej republiky
ÚOOÚ SR - Úrad na ochranu osobných údajov SR
ÚNMS SR - Úrad pre normalizáciu, metrológiu a skúšobníctvo SR
ÚPREKaPS - Úrad pre reguláciu elektronických komunikácií a poštových služieb
VS - Vojenské spravodajstvo
ZMOS - Združenie miest a obcí Slovenska