



NÁRODNÝ  
BEZPEČNOSTNÝ  
ÚRAD

# ODPOČET IMPLEMENTÁCIE AKČNÉHO PLÁNU

realizácie Národnej stratégie  
kybernetickej bezpečnosti  
na roky 2021 až 2025





# Obsah

Všeobecné úlohy k stratégii	4
Dôveryhodný štát pripravený na hrozby	5
Efektívne odhaľovanie a objasňovanie počítačovej kriminality	12
Odoľný súkromný sektor	19
Kybernetická bezpečnosť ako základná súčasť verejnej správy	21
Silné partnerstvá	23
Vzdelaní odborníci a vzdelaná verejnosť	30
Výskum a vývoj v oblasti kybernetickej bezpečnosti	41

## Všeobecné úlohy k stratégii

Kód úlohy	Úloha	Popis úlohy	Zodpovedný subjekt	Súčinný subjekt	Časový horizont realizácie	Návrh merateľných ukazovateľov	Stav plnenia	Spôsob plnenia	Dôkaz
Z.3	<b>Odpočet plnenia Akčného plánu</b>	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	Pravidelná správa o plnení úloh Akčného plánu za príslušné obdobie predložená do výboru	Priebežne plnené	Zaslané odpočty od zodpovedných subjektov	Odpočty zaslané predsedovi Monitorovacieho výboru, premietnuté do odpočtu za rok 2022
Z.4	<b>Vypracovanie pravidelnej ročnej správy o plnení úloh Akčného plánu</b>	Vypracovať priebežnú správu o plnení úloh Akčného plánu a predložiť ho riaditeľovi NBÚ vždy do konca januára zo strany monitorovacieho výboru	Monitorovací výbor		Priebežne	Pravidelná ročná správa schválená monitorovacím výborom predložená riaditeľovi NBÚ	Priebežne plnené	Sumár odpočtov v ročnej správe o KB	Ročná správa o KB
Z.5	<b>Financovanie úloh – merateľné ukazovatele</b>	Pripraviť a vyhlásiť dopytové výzvy na financovanie úloh Akčného plánu prostredníctvom operačných programov fondov Európskeho spoločenstva, fondu obnovy a iných foriem financovania bez vplyvu na štátny rozpočet	MIRRI SR, MF SR		Priebežne	<ul style="list-style-type: none"> <li>Počet úloh s vytvoreným financovaním</li> <li>počet zrealizovaných projektov naviazaných na úlohy z akčného plánu</li> <li>objem finančných prostriedkov naviazaných na úlohy z Akčného plánu.</li> </ul>	Priebežne plnené	MF SR v roku 2022 nevyhlásil dopytové výzvy na financovanie úloh Akčného plánu, nakoľko nie je gestor relevantných operačných programov. MIRRI SR počas roka 2022 financovalo projekty na podporu rozvoja kybernetickej a informačnej bezpečnosti (vid dôkaz)	<ul style="list-style-type: none"> <li><a href="https://www.mirri.gov.sk/projekty/projektyesif/operacny-program-integrovanainfrastruktura/prioritna-os-7-informacnaspolocnost/vyzvania-a-vyzvy/vyzvac-opii-2021-7-16/index.html">https://www.mirri.gov.sk/projekty/projektyesif/operacny-program-integrovanainfrastruktura/prioritna-os-7-informacnaspolocnost/vyzvania-a-vyzvy/vyzvac-opii-2021-7-16/index.html</a></li> <li><a href="https://www.mirri.gov.sk/projekty/projektyesif/operacny-program-integrovanainfrastruktura/prioritna-os-7-informacnaspolocnost/vyzvania-a-vyzvy/vyzvac-opii-2022-7-20-dop-governanc/index.html">https://www.mirri.gov.sk/projekty/projektyesif/operacny-program-integrovanainfrastruktura/prioritna-os-7-informacnaspolocnost/vyzvania-a-vyzvy/vyzvac-opii-2022-7-20-dop-governanc/index.html</a></li> </ul>

# Dôveryhodný štát pripravený na hrozby

Kód úlohy	Úloha	Popis úlohy	Zodpovedný subjekt	Súčinný subjekt	Časový horizont realizácie	Návrh merateľných ukazovateľov	Stav plnenia	Spôsob plnenia	Dôkaz
A.1	<b>Novela vyhlášky o identifikačných kritériách</b>	Pripraviť a zabezpečiť schválenie novely vyhlášky, ktorou sa určujú identifikačné kritériá prevádzkovej služby (kritériá základnej služby)	NBÚ	Ústredné orgány štátnej správy, PZS, odborná verejnosť, SIS	12/2021	Aktualizovaná vyhláška o identifikačných kritériách prevádzkovej služby (kritériá základnej služby) predložená do medzirezortného pripomienkového konania	Plní sa	NBÚ pracuje na novele vyhlášky, momentálne prebiehajú interné diskusie	
A.2	<b>Novela vyhlášky o kategóriách incidentov</b>	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	Aktualizovaná vyhláška o identifikačných kritériách pre jednotlivé kategórie KBI a podrobnosti hlásenia KBI predložená do medzirezortného pripomienkového konania	Plní sa	Vyhláška pripravená na zaslanie do komunity na pripomienkovanie. Následne bude predložená do MPK	
A.3	<b>Politiky</b>	Vytvorenie ekonomického modelu politik v oblasti kybernetickej bezpečnosti v Slovenskej republike	NBÚ	SIS, MF SR, MIRRI SR	12/2022	Vytvorenie ekonometrického modelu a systému na jeho aplikáciu	Plní sa	Vytvorenie ekonometrického modelu je vo fáze prípravy zo strany NBÚ	
A.5	<b>Posúdenie rizík</b>	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	06/2022	Publikovanie schválenej metodiky pre posúdenie rizík sektorov, vybraných technológií a služieb	Splnené	Metodika bola zverejnená na webe NBÚ, pričom pri sektorovom posúdení rizík budú vzaté do úvahy špecifiká jednotlivých sektorov	<a href="https://www.nbu.gov.sk/kybernetickabezpecnost/riadenie-rizik/index.html">https://www.nbu.gov.sk/kybernetickabezpecnost/riadenie-rizik/index.html</a>

Dôveryhodný štát pripravený na hrozby – tabuľka 1/7

Kód úlohy	Úloha	Popis úlohy	Zodpovedný subjekt	Súčinný subjekt	Časový horizont realizácie	Návrh merateľných ukazovateľov	Stav plnenia	Spôsob plnenia	Dôkaz
A.6	<b>Prvé posúdenie rizík</b>	Vykonať prvé sektorové posúdenie rizík	NBÚ	Sektorové ústredné orgány	12/2022	Vykonanie posúdenia rizík vo vybraných sektoroch	Plní sa	NBÚ pripravuje prvé posúdenia rizík, momentálne prebiehajú interné diskusie o spôsobe vykonania a sektoroch.	
A.7	<b>Priebežné posúdenie rizík</b>	Najmenej jedenkrát ročne aktualizovať sektorové posúdenie rizík	NBÚ	Sektorové ústredné orgány	12/2022 a následne raz ročne	1× ročne aktualizácia sektorového posúdenia rizík	Plní sa	NBÚ pripravuje prvé posúdenia rizík, momentálne prebiehajú interné diskusie o spôsobe vykonania a sektoroch.	
A.8	<b>Sektorové vyhlášky</b>	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	Počet návrhov vyhlášok (ktorými sa ustanovia sektorové bezpečnostné opatrenia pre podsektor Bezpečnosť sektora Verejná správa podľa zákona o kybernetickej bezpečnosti) predložených do legislatívneho procesu“	Plní sa	MV SR: MV SR (SITB MV SR) vykonalo analýzu potrieb a požiadaviek sektora č. 10 – Verejná správa, podsektora – Bezpečnosť, ktorého je gestorom. Výsledky analýzy mali byť východiskom pre prípravu podkladov na vypracovanie návrhu všeobecne záväzného právneho predpisu, ktorý mal ustanoviť sektorové bezpečnostné opatrenia pre sektor č. 10 – Verejná správa, podsektor – Bezpečnosť. Výsledkom analýzy je konštatovanie MV SR, ako ústredného orgánu a gestora podsektora Bezpečnosť, že nie je potreba ustanovovať a prijímať špecifické sektorové bezpečnostné opatrenia, nakoľko plne postačujú všeobecné bezpečnostné opatrenia upravené vo vyhláške NBÚ č. 362/2018 Z. z. Uvedené sa potvrdilo aj pri výkone auditov kybernetickej bezpečnosti. MD SR: MD SR vykonalo analýzu potrieb a požiadaviek sektorov Doprava, Pošta, Elektronické komunikácie ktorých je gestorom. Na základe analýzy boli definované sektorové kritériá, ktoré sú východiskom pre prípravu podkladov na vypracovanie návrhu sektorových vyhlášok, ktoré ustanovia sektorové bezpečnostné opatrenia pre predmetné	

Kód úlohy	Úloha	Popis úlohy	Zodpovedný subjekt	Súčinný subjekt	Časový horizont realizácie	Návrh merateľných ukazovateľov	Stav plnenia	Spôsob plnenia	Dôkaz
A. 10	<b>Detekcia a zber</b>	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, algoritmi a technológiami, vrátane umelej inteligencie	NBÚ	SIS, VS	Priebežne	Počet detegovaných udalostí, počet detegovaných incidentov a počet riešených incidentov	Priebežne plnené	Počty detegovaných udalostí, incidentov a počty riešených incidentov sú podrobne uvedené v ročnej správe o KB	Ročná správa o KB
A. 11	<b>Atribúcia</b>	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	Vytvorenie procesu technickej a politickej atribúcie	Plní sa	NBÚ pripravuje proces atribúcie, momentálne prebieha interné pripomienkovanie.	
A. 12	<b>Varovania</b>	Priebežne vytvárať a zverejňovať varovania pred technologickými zraniteľnosťami a problematickými aktivitami v kybernetickom priestore, vrátane adresných varovaní konkrétnym subjektom	NBÚ		Priebežne	Počet vytvorených a zverejňovaných varovaní	Priebežne plnené	Počet vydaných varovaní sa nachádza v ročnej správe o KB	Ročná správa o KB
A. 13	<b>Verejnosť</b>	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	Počet verejných workshopov, konferencií, okrúhlych stolov s účasťou zástupcov NBÚ a sektorových ústredných orgánov	Priebežne plnené	<ul style="list-style-type: none"> <li>NBÚ: aktívna účasť na národných konferenciách (EPI, ITAPA, Qubit a iné)</li> <li>MFSR: účasť na konferenciách Nová stratégia kybernetickej bezpečnosti EÚ – smernica NIS 2, Aktuálne kybernetické hrozby, ako sa na ne pripraviť, Sectec security day, ITAPA</li> <li>MDV SR: Účasť na 2 workshopoch ku KB</li> </ul>	

Dôveryhodný štát pripravený na hrozby – tabuľka 3/7

Kód úlohy	Úloha	Popis úlohy	Zodpovedný subjekt	Súčinný subjekt	Časový horizont realizácie	Návrh merateľných ukazovateľov	Stav plnenia	Spôsob plnenia	Dôkaz
A.14	<b>CSIRT</b>	Podporovať vznik špecializovaných pracovísk typu CSIRT na území SR	NBÚ		Priebežne	Počet vzniknutých CSIRT jednotiek na území SR s minimálne statusom „Listed“ v organizácii Trusted Introducer	Priebežne plnené	<ul style="list-style-type: none"> <li>Počet CSIRT jednotiek so statusom „Listed“ v TI: 4</li> <li>Počet CSIRT jednotiek so statusom „Accredited“ v TI: 7</li> <li>Počet CSIRT jednotiek so statusom „Certified“ v TI: 1</li> <li>Počet CSIRT jednotiek vo FIRST: 3</li> </ul>	Databázy Trusted Introducer a FIRST
A.15	<b>Budovanie spôsobilostí v oblasti obrany</b>	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	<ul style="list-style-type: none"> <li>Aktualizácia príslušnej národnej a rezortnej legislatívy;</li> <li>Spracovanie strategických a doktrinálnych materiálov; a</li> <li>Zavádzanie novej techniky a zbraňových systémov</li> </ul>	Priebežne plnené	Vstup do platnosti – Zákon č. 500/2022 Z. z. o Vojenskom spravodajstve (02/2023) Schválenie Stratégie kybernetickej obrany SR (05/2022); Schválenie Akčného plánu implementácie Stratégie kybernetickej obrany SR (11/2022); Participácia na aktualizovaní rezortných strategických dokumentov týkajúcich sa obrany štátu; a Spracovávanie interných služobných pomôcok zameraných na štandardizáciu postupov.	Zákon č. 500 /2022 Z. z. – <a href="https://www.slovlex.sk/pravnepredpisy/SK/ZZ/2022/500/20230201">https://www.slovlex.sk/pravnepredpisy/SK/ZZ/2022/500/20230201</a> Stratégia KO – <a href="https://www.slovlex.sk/legislativneprocesy/SK/LP/2022/128">https://www.slovlex.sk/legislativneprocesy/SK/LP/2022/128</a> Akčný plán KO – <a href="https://rokovania.gov.sk/RVL/Material/27883/1">https://rokovania.gov.sk/RVL/Material/27883/1</a> Rezortné materiály a služobné pomôcky – nie je možné zverejniť nakoľko ide o utajované skutočnosti v zmysle Zákona č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov.



Kód úlohy	Úloha	Popis úlohy	Zodpovedný subjekt	Súčinný subjekt	Časový horizont realizácie	Návrh merateľných ukazovateľov	Stav plnenia	Spôsob plnenia	Dôkaz
A. 16	<b>Budovanie spôsobilostí v oblasti obrany</b>	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	<ul style="list-style-type: none"> <li>Participácia na príprave nových interných predpisov obranného plánovania;</li> <li>Inkorporovanie kybernetickej domény a operácií do príslušných rozpočtových kapitol rezortu obrany;</li> <li>Inkorporovanie aliančného obranného plánovania do národných podmienok; a</li> <li>Participácia na činnosti príslušných rezortných pracovných skupín.</li> </ul>	<b>Splnené</b>	<p>Participácia na príprave príslušných rezortných dokumentov – Smernice Metodiky a pod.;Príprava Cieľov síl NATO 2021; a Participácia na činnosti EÚ – CARD.</p>	<p>Plnenie cieľov E6202, interné smernice, metodiky a plány podliehajú režimu utajenia. Proces koordinovaného výročného preskúmania v oblasti obrany (CARD) – <a href="https://www.mosr.sk/46746-sk/pesco/">https://www.mosr.sk/46746-sk/pesco/</a></p>
A. 17	<b>Budovanie spôsobilostí v oblasti spravodajstva</b>	Pokračovať v budovaní, nastavovaní, posilňovaní a udržiavaní plnohodnotných spôsobilostí kybernetického spravodajstva, zlepšovať technické aj personálne spôsobilosti.	SIS	NBÚ, VS	Priebežne	Odpočet aktivít	<b>Priebežne plnené</b>	<p>Slovenská informačná služba v roku 2022 pokračovala v realizácii krokov smerujúcich k plneniu úlohy A.17 z Akčného plánu Národnej stratégie kybernetickej bezpečnosti. Boli vykonané také organizačné opatrenia, ktoré majú potenciál prispieť k plánovanému plneniu úloh v oblasti kybernetického spravodajstva. V podmienkach Slovenskej informačnej služby bol vytvorený priestor na zabezpečenie adekvátnej odbornej spôsobilosti príslušníkov pôsobiacich v predmetnej oblasti, čím je možné dosiahnuť plnenie stanovených úloh na požadovanej úrovni. Výzvou naďalej ostáva personálne naplnenie súvisiacich kapacít Slovenskej informačnej služby tak, aby bolo zabezpečené kontinuálne plnenie úloh na úseku kybernetického spravodajstva. Tu je potrebné aj naďalej vytvárať podmienky na získanie a udržanie odborne spôsobilého personálu, vrátane zabezpečenia jeho adekvátneho finančného ohodnotenia. Napriek limitujúcim faktorom plynúcim z pridelených rozpočtových prostriedkov Slovenská informačná služba v roku 2022 vykonala aj potrebné kroky s cieľom zlepšenia technických spôsobilostí v oblasti kybernetickej bezpečnosti a kybernetického spravodajstva. Bola konzultovaná a nastavovaná vhodná úroveň kooperácie úsekov kybernetického spravodajstva a kybernetickej bezpečnosti, najmä so zriadenou jednotkou CSIRT SIS, a to nielen za účelom dosiahnutia vyššej úrovne</p>	

Dôveryhodný štát pripravený na hrozby – tabuľka 5/7

Kód úlohy	Úloha	Popis úlohy	Zodpovedný subjekt	Súčinný subjekt	Časový horizont realizácie	Návrh merateľných ukazovateľov	Stav plnenia	Spôsob plnenia	Dôkaz
A.22	<b>Certifikácia výrobkov, procesov a služieb v oblasti kybernetickej bezpečnosti</b>	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	Rozhodnutie o akreditácii	Nesplnené	EK doteraz neschválila certifikačné schémy. Bez toho nie je možné spustiť akreditáciu.	
A.23	<b>Budovanie spôsobilostí na audit kybernetickej bezpečnosti</b>	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 17024)“, na základe doterajších praktických skúseností.	NBÚ	KCCKB	12/2022	Publikovaná aktualizovaná certifikačná schéma	Plní sa	Prebieha príprava aktualizácie certifikačnej schémy pre certifikáciu audítorov KB	
A.24	<b>Budovanie spôsobilostí v riadení kybernetickej bezpečnosti</b>	Dosiahnuť akreditáciu pre certifikáciu manažérov kybernetickej bezpečnosti podľa osobitného predpisu a podľa normy STN EN ISO/IEC 17024	KCCKB	SNAS	12/2021	Rozhodnutie o akreditácii	Splnené	Bolo vydané rozhodnutie o akreditácii pre certifikáciu manažérov KB pre KCCKB	<a href="https://cybercompetence.sk/kompetencnecentrum-certifikuje-manazerovkyberbezpecnosti/">https://cybercompetence.sk/kompetencnecentrum-certifikuje-manazerovkyberbezpecnosti/</a>
A.27	<b>Posudzovanie zhody v kybernetickej bezpečnosti</b>	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 posudzovania zhody	priebežne	Publikovaná národná certifikačná schéma	Neodpočítované		

Kód úlohy	Úloha	Popis úlohy	Zodpovedný subjekt	Súčinný subjekt	Časový horizont realizácie	Návrh merateľných ukazovateľov	Stav plnenia	Spôsob plnenia	Dôkaz
A. 28	<b>Podpora spôsobilostí subjektov v oblasti riadenia kontinuity činností</b>	Vytvoriť rámec pre oblasti riadenia kontinuity činností a havarijného plánovania v kybernetickej bezpečnosti	NBÚ		06/2022	Publikovaná metodika BCM	Plní sa	NBÚ pripravuje rámec pre BCM, momentálne prebieha interná diskusia.	
A. 29	<b>Vytvorenie komunity kybernetickej bezpečnosti</b>	Efektívna spolupráca zainteresovaných strán na všetkých úrovniach riešenia kybernetickej bezpečnosti s dôrazom na mimovládne organizácie	NBÚ	Ústredné orgány, KCCKB, záujmové zväzy, združenia a asociácie v oblasti kybernetickej bezpečnosti	12/2021	Zriadenie a akreditácia NCC	Splnené	NCC bolo zriadené a akreditované	www.kyberkomunita.sk
A. 30	<b>Návrh indexu pre oblasť kybernetickej bezpečnosti a jeho pravidelné vyhodnocovanie</b>	Navrhnuť 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	Metodika na vypracovanie pravidelného merania stavu pre oblasť kybernetickej bezpečnosti v SR	Plní sa	NBÚ pripravil návrh indexu pre oblasť KB, momentálne prebieha interné pripomienkovanie a metodika bude následne zaslaná komunite na pripomienkovanie.	

Dôveryhodný štát pripravený na hrozby – tabuľka 7/7

# Efektívne odhaľovanie a objasňovanie počítačovej kriminality

Kód úlohy	Úloha	Popis úlohy	Zodpovedný subjekt	Súčinný subjekt	Časový horizont realizácie	Návrh merateľných ukazovateľov	Stav plnenia	Spôsob plnenia	Dôkaz
B.1	<b>Zefektívnenie NES</b>	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	<ul style="list-style-type: none"> <li>Vykonal analýzu zefektívnenia fungovania Národnej expertnej skupiny na riešenie problematiky v oblasti počítačovej kriminality</li> <li>Implementácia záverov analýzy do praxe prijatím konkrétnych opatrení</li> </ul>	Plní sa	Analýza zefektívnenia fungovania Národnej expertnej skupiny na riešenie problematiky v oblasti počítačovej kriminality bola v roku 2021 realizovaná (OPK ÚKP P PZ) priebežne, a to v priebehu konania zasadnutí zameraných na konkrétne riešenie problematiky.	Záznamy z jednotlivých stretnutí
B.2	<b>Rozvoj spolupráce s vybranými vysokými školami v oblasti počítačovej kriminality</b>	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 problematike (aktivity ako pravidelné prednášky, vedenie špecializovaných predmetov, vedenie záverečných prác, prepojenie teórie s praxou a podobne)			07/2022	<ul style="list-style-type: none"> <li>Vytvorenie programu spolupráce a vzdelávania na vybraných vysokých školách v oblasti počítačovej kriminality</li> <li>Počet zrealizovaných aktivít v rámci implementácie programu</li> </ul>	Plní sa	<ul style="list-style-type: none"> <li>MV SR (APZ) je aktívne v oblasti počítačovej kriminality vo viacerých úrovniach. Problematika počítačovej kriminality je preberaná vo výučbe v bakalárskom ako aj magisterskom stupni vysokoškolského vzdelávania v podobe prednášok v predmetoch vyučovaných katedrami cez rôzne uhly pohľadov</li> <li>V rámci prípravy podkladov pre novú akreditáciu študijných odborov pre Slovenskú akreditačnú agentúru, ako aj z dôvodu potreby systemizácie výučby počítačovej kriminality, je plánovaná posilnená časová dotácia v rôznych predmetoch, zaradenie nových tém na prednáškach, seminároch a cvičeniach a v neposlednom rade aj vytvorenie nového predmetu pod názvom Základy počítačovej kriminality</li> <li>Téma počítačovej kriminality je spracovávaná aj formou vypisovania tém záverečných prác (bakalárskych, magisterských a doktorandských) ako aj prác, spracovávaných v rámci študentskej vedeckej a odbornej činnosti</li> </ul>	

Kód úlohy	Úloha	Popis úlohy	Zodpovedný subjekt	Súčinný subjekt	Časový horizont realizácie	Návrh merateľných ukazovateľov	Stav plnenia	Spôsob plnenia	Dôkaz
B.3	<b>Príprava vzdelávacích programov pre justičné orgány</b>	Vytvoriť koncept systematického špecializovaného a interdisciplinárneho vzdelávania právnych čakaateľov 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	Splnenie úlohy schválením Študijného plánu Justičnej akadémie SR narok 2022	Plní sa	Schválený študijný plán	
B.4	<b>Systematické vzdelávanie justičných orgánov</b>	Na základe vytvoreného konceptu systematicky vzdelávať právnych čakaateľov 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	2 × ročne	Systematické vzdelávanie justičných orgánov v oblasti boja proti počítačovej kriminalite 2 × ročne	Priebežne plnené	Online vzdelávanie: Počítačová kriminalita II. (58 účastníkov)	Sp. zn. 2022/KVP/135/OP EVS
B.5	<b>Koncept vzdelávania policajtov</b>	Vytvoriť koncept špecialistov pre počítačovú kriminalitu na úrovni základných útvarov, vyšetrovania a kriminalisticko-expertíznych činností a ich pravidelného vzdelávania	MV SR		12/2021	<ul style="list-style-type: none"> <li>Vytvorenie konceptu vzdelávania špecialistov pre počítačovú kriminalitu</li> <li>Počet zrealizovaných vzdelávacích aktivít pre špecialistov na počítačovú kriminalitu</li> </ul>	Plní sa	MV SR (OPK ÚKP P PZ) vytvorilo nový, aktualizovaný zoznam policajtov výkonných útvarov v rámci jednotlivých okresných a krajských riaditeľstiev Policajného zboru, ktorí sú priebežne preškoľovaní z problematiky počítačovej kriminality, či už vo všeobecnej rovine, alebo z niektorej zo špecifických oblastí počítačovej kriminality.	

Efektívne odhaľovanie a objasňovanie počítačovej kriminality – tabuľka 2/7

Kód úlohy	Úloha	Popis úlohy	Zodpovedný subjekt	Súčinný subjekt	Časový horizont realizácie	Návrh merateľných ukazovateľov	Stav plnenia	Spôsob plnenia	Dôkaz
B.6	<b>Implementácia konceptu vzdelávania policajtov</b>	Pravidelne uskutočňovať základné a rozšírené kurzy boja proti počítačovej kriminalite podľa konceptu vzdelávania špecialistov pre počítačovú kriminalitu so zameraním sa na špecifiká zaistovania stôp, prípravného konania a operatívnych postupov, s frekvenciou minimálne 3 × ročne/kurz	MV SR		3 × ročne	<ul style="list-style-type: none"> <li>Počet zrealizovaných základných kurzov boja proti počítačovej kriminalite</li> <li>Počet policajtov zúčastnených na realizovaných základných kurzoch</li> <li>Počet zrealizovaných rozšírených kurzov boja proti počítačovej kriminalite</li> <li>Počet policajtov zúčastnených na realizovaných rozšírených kurzoch</li> </ul>	Priebežne plnené	V rámci MV SR (OPK NCODK P PZ) boli podľa čl. 21 ods. 2 nariadenia ministra vnútra Slovenskej republiky č. 153/2011 o odbornom vzdelávaní príslušníkov Policajného zboru akreditované 2 kurzy počítačovej kriminality (1 základný a 1 zdokonaľovací).	Vytvorenie nového, aktualizovaného zoznamu policajtov výkonných útvarov v rámci jednotlivých okresných a krajských riaditeľstiev Policajného zboru, ktorí sú priebežne preškoľovaní z problematiky počítačovej kriminality, online školenie pre policajtov okresných a krajských riaditeľstiev Policajného zboru na tému „Počítačová kriminalita, špecifiká odhaľovania trestnej činnosti detskej pornografie“.

Efektívne odhaľovanie a objasňovanie počítačovej kriminality – tabuľka 3/7

Kód úlohy	Úloha	Popis úlohy	Zodpovedný subjekt	Súčinný subjekt	Časový horizont realizácie	Návrh merateľných ukazovateľov	Stav plnenia	Spôsob plnenia
B.7	<b>Prehodnocovanie a prispôbovanie kurzov počítačovej kriminality</b>	Pravidelne prehodnocovať kurzy boja proti počítačovej kriminalite pre príslušníkov PZ a prispôbovanie osnov podľa aktuálnych potrieb, ktoré vzniknú na základe analýzy bezpečnostného prostredia	MV SR		najmenej 1× ročne	Aktualizácia vzdelávacích osnov pre kurzy boja proti počítačovej kriminalite	<b>Priebežne plnené</b>	Ministerstvo vnútra Slovenskej republiky (OPK NCODK P PZ) organizuje základný kurz počítačovej kriminality a zdokonaľovací kurz počítačovej kriminality, ktoré boli akreditované podľa čl. 21 ods. 2 nariadenia ministra vnútra Slovenskej republiky č. 153/2011 o odbornom vzdelávaní príslušníkov Policajného zboru. Oba kurzy majú v rámci organizačných podmienok uskutočňovania kurzov schválenú možnosť upravovať obsah a štruktúru učebného plánu a učebných osnov v rozsahu maximálne 10 % počtu vyučovacích hodín, pričom nesmie byť prekročený celkový počet hodín kurzu. Úpravy nad uvedený rámec sú podmienené inovovaním vzdelávacieho projektu a jeho opakovanou akreditáciou v Akreditačnej komisii Ministerstva vnútra Slovenskej republiky pre policajné vzdelávanie. Aktualizácia vzdelávacích osnov je realizovaná priebežne za dodržania vyššie uvedenej podmienky. Týmto spôsobom sú najčastejšie aktualizované techniky a postupy na odhaľovanie, objasňovanie a vyšetrovanie počítačovej kriminality a to tak, aby reflektovali na najnovšie trendy a vývoj počítačovej kriminality. aktualizované techniky a postupy na odhaľovanie, objasňovanie a vyšetrovanie počítačovej kriminality v rámci základného kurzu počítačovej kriminality a to tak, aby reflektovali na najnovšie trendy a vývoj počítačovej kriminality
								<b>Dôkaz</b> Aktualizované techniky a postupy na odhaľovanie, objasňovanie a vyšetrovanie počítačovej kriminality v rámci základného kurzu počítačovej kriminality a to tak, aby reflektovali na najnovšie trendy a vývoj počítačovej kriminality

**Efektívne odhaľovanie a objasňovanie počítačovej kriminality – tabuľka 4/7**

Kód úlohy	Úloha	Popis úlohy	Zodpovedný subjekt	Súčinný subjekt	Časový horizont realizácie	Návrh merateľných ukazovateľov	Stav plnenia	Spôsob plnenia	Dôkaz
B.8	<b>Podanie žiadosti o zápis znaleckého ústavu</b>	Podat' 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	Zápis v zozname znalcov	Nesplnené	MSSR v súčasnosti finalizuje vyhlášku 228/2018 Z. z. Rozšíri sa tým zoznam znaleckých odvetví. Na znalecký ústav je nutná spolupráca s VŠ. Dohoda je s FIIT STU. Následne žiadosť o zápis znaleckého ústavu	
B.9	<b>Koncept vzdelávania znalcov</b>	Vytvoriť koncept vzdelávania znalcov v oblasti počítačovej kriminality so zameraním sa najmä na analýzu a vyhodnocovanie digitálnych stôp	KCCKB	znalecké ústavy	06/2022	Publikované sylaby	Nesplnené	MSSR v súčasnosti finalizuje vyhlášku 228/2018 Z. z. Rozšíri sa tým zoznam znaleckých odvetví o nové odvetvie kybernetická bezpečnosť. Následne koncept	
B.10	<b>Implementácia konceptu vzdelávania znalcov</b>	Na základe vytvoreného konceptu systematicky vzdelávať znalcov v oblasti počítačovej kriminality s frekvenciou minimálne 3 × ročne/kurz	KCCKB	znalecké ústavy	3 × ročnew	Schéma vzdelávania KCCKB rozšírená o sylaby vzdelávania znalcov	Nesplnené	MSSR v súčasnosti finalizuje vyhlášku 228/2018 Z. z. Rozšíri sa tým zoznam znaleckých odvetví o nové odvetvie kybernetická bezpečnosť. Následne koncept. Následne vzdelávací produkt	
B.11	<b>Zefektívnenie zabezpečovania užívateľských údajov pre trestné konanie</b>	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		Neodpočítané		



Kód úlohy	Úloha	Popis úlohy	Zodpovedný subjekt	Súčinný subjekt	Časový horizont realizácie	Návrh merateľných ukazovateľov	Stav plnenia	Spôsob plnenia	Dôkaz
B. 12	<b>Odstránenie legislatívnych prekážok</b>	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	Vykonanie analýzy stavu aplikačnej praxe pri vyšetrowaní trestných činov počítačovej kriminality a návrh prípadných legislatívnych zmien	Plní sa	Ministerstvo vnútra Slovenskej republiky (OPK ÚKP P PZ) vykonalo v rámci prípravy novely trestného kódexu (Trestného zákona a Trestného poriadku) analýzu stavu aplikačnej praxe pri vyšetrowaní trestných činov počítačovej kriminality a spracovalo návrh potrebných legislatívnych zmien	Návrhy v rámci novely Trestného zákona
B. 13	<b>Implementácia zistení</b>	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		Neodpočítavané		Návrhy v rámci novely Trestného zákona

Efektívne odhaľovanie a objasňovanie počítačovej kriminality – tabuľka 6/7

Kód úlohy	Úloha	Popis úlohy	Zodpovedný subjekt	Súčinný subjekt	Časový horizont realizácie	Návrh merateľných ukazovateľov	Stav plnenia	Spôsob plnenia	Dôkaz
B. 17	<b>Zefektívnenie zaistovania elektronických stôp</b>	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	<ul style="list-style-type: none"> <li>Počet kriminalistických technikov preškolených z oblasti počítačovej kriminality</li> <li>Aktualizácia postupov v rámci expertíznej činnosti</li> <li>Počet súdnych znalcov v príslušnom odbore prizývaných k prípadom počítačovej kriminality</li> </ul>	Plní sa	MV SR (OPK NCODK P PZ) pravidelne analyzuje a vyhodnocuje vývoj a trendy v oblasti počítačovej kriminality, na základe ktorých vypracováva a aktualizuje metodické pomôcky a usmernenia určené pre policajtov služby kriminálnej polície, poverených príslušníkov a vyšetrovateľov, ktorí vykonávajú odhaľovanie, objasňovanie a vyšetrovanie počítačovej kriminality. Tieto metodické pomôcky a usmernenia sú sprístupnené na intranetovom webovom sídle príslušného špecializovaného útvaru Ministerstva vnútra Slovenskej republiky	V roku 2022 bolo aktualizovaných nasledovných 5 metodických pomôcok a usmernení: Metodické usmernenie k postupu útvarov Policajného zboru pri zisťovaní používateľov internetových služieb Metodické usmernenie k postupu útvarov Policajného zboru pri predkladaní žiadosti o urýchlené uchovanie uložených počítačových údajov podľa Dohovoru o počítačovej kriminalite Metodické usmernenie k sieťovému prekladu IP adries (NAT) a vyžadovaniu informácií od poskytovateľov internetového pripojenia Metodika k spracovávaniu informácií zasielaných prostredníctvom Národného centra pre nezvestné a vykorisťované deti (NCMEC) Metodická pomôcka k získavaniu základných identifikátorov na sociálnej sieti Facebook
B. 18	<b>Rozvoj metodickej činnosti</b>	Pravidelne analyzovať, prehodnocovať a rozvíjať metodickú činnosť v oblasti počítačovej kriminality so zameraním sa na vydávanie metodických pomôcok a usmernení			Priebežne	Počet vydaných metodických pomôcok a usmernení	Priebežne plnené	MV SR (OPK NCODK P PZ) pravidelne analyzuje a vyhodnocuje vývoj a trendy v oblasti počítačovej kriminality, na základe ktorých vypracováva a aktualizuje metodické pomôcky a usmernenia určené pre policajtov služby kriminálnej polície, poverených príslušníkov a vyšetrovateľov, ktorí vykonávajú odhaľovanie, objasňovanie a vyšetrovanie počítačovej kriminality. Tieto metodické pomôcky a usmernenia sú sprístupnené na intranetovom webovom sídle príslušného špecializovaného útvaru Ministerstva vnútra Slovenskej republiky	V roku 2022 bolo aktualizovaných nasledovných 5 metodických pomôcok a usmernení: Metodické usmernenie k postupu útvarov Policajného zboru pri zisťovaní používateľov internetových služieb, Metodické usmernenie k postupu útvarov Policajného zboru pri predkladaní žiadosti o urýchlené uchovanie uložených počítačových údajov podľa Dohovoru o počítačovej kriminalite, Metodické usmernenie k sieťovému prekladu IP adries (NAT) a vyžadovaniu informácií od poskytovateľov internetového pripojenia, Metodika k spracovávaniu informácií zasielaných prostredníctvom Národného centra pre nezvestné a vykorisťované deti (NCMEC) Metodická pomôcka k získavaniu základných identifikátorov na sociálnej sieti Facebook

# Odolný súkromný sektor

Kód úlohy	Úloha	Popis úlohy	Zodpovedný subjekt	Súčinný subjekt	Časový horizont realizácie	Návrh merateľných ukazovateľov	Stav plnenia	Spôsob plnenia	Dôkaz
C.1	<b>Tréningy a cvičenia pre súkromný sektor</b>	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	3× ročne	Správy z cvičení	Priebežne plnené	V roku 2022 zorganizovaná kyberbezpečnostná hra CyberGame, ktorá trvala 10 týždňov a bola určená širokému okruhu adresátov, vrátane PZS	www.cybergame.sk
C.2	<b>Vytvorenie inkubátorov kybernetickej bezpečnosti</b>	Pripraviť právny rámec pre vytvorenie inkubátorov kybernetickej bezpečnosti pre malé firmy (startupy) a prepojiť tak vedu a výskum so súkromným sektorom a podporovať vznik inovácií v oblasti kybernetickej bezpečnosti	MH SR	MF SR, MIRRI SR, NBÚ	01/2022	Existencia právneho rámca pre vytvorenie inkubátorov kybernetickej bezpečnosti pre malé firmy	Neodpočítavané		
C.3	<b>Dotačné schémy pre prevádzkovateľov základných služieb</b>	Vytvoriť a udržiavať dotačné schémy pre prevádzkovateľov základných služieb zameraných na budovanie spôsobilostí v oblasti kybernetickej bezpečnosti	MH SR	MF SR, MIRRI SR	01/2022	Súbor vypracovaných dotačných schém pre prevádzkovateľov základných služieb v zmysle popisu úlohy vrátane konkrétne definovaného finančného zabezpečenia jednotlivých dotačných schém	Neodpočítavané		

Odolný súkromný sektor – tabuľka 1/2

Kód úlohy	Úloha	Popis úlohy	Zodpovedný subjekt	Súčinný subjekt	Časový horizont realizácie	Návrh merateľných ukazovateľov	Stav plnenia	Spôsob plnenia	Dôkaz
C.4	<b>Harmonizácia pravidiel pre hlásenie incidentov</b>	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, ÚPRE-KaPS	01/2022	Vytvorenie modelu, ktorý zjednotí hlásenie incidentov	Plní sa	NBÚ v spolupráci so súčinnosťnými subjektami pripravuje zjednotenie hlásenia incidentov. Momentálne prebiehajú diskusie o spôsobe, ako zjednotiť jednotlivé hlásenia.	
C.6	<b>Vytvorenie platformy výmeny informácií v oblasti kybernetickej bezpečnosti</b>	Vytvoriť platformu pre efektívnu spoluprácu, zdieľanie informácií a odbornú diskusiu verejného sektora so súkromným sektorom v oblasti kybernetickej bezpečnosti	NBÚ	PZS	12/2021	Spustenie systému, vydaný štatút platformy a vydaná metodika činnosti	Plní sa	Takáto platforma bude vytvorená v rámci pracovných skupín NCC	<a href="https://www.kyberkomunita.sk/pracovneskupiny/">https://www.kyberkomunita.sk/pracovneskupiny/</a>

# Kybernetická bezpečnosť ako základná súčasť verejnej správy

Kód úlohy	Úloha	Popis úlohy	Zodpovedný subjekt	Súčinný subjekt	Časový horizont realizácie	Návrh merateľných ukazovateľov	Stav plnenia	Spôsob plnenia	Dôkaz
D.1	<b>Zjednotenie postupov a bezpečnostných opatrení a kontinuálne presadzovanie ich implementácie vo verejnej správe</b>	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	Hodnota ukazovateľa: Splnená/nesplnená	Plní sa	Plnené priebežne. MIRRI SR na svojom webovom sídle priebežne zverejňuje a aktualizuje metodické usmernenia pre implementáciu týchto opatrení. Predpokladaný termín dokončenia úlohy: 12/2024	<a href="https://www.mirri.gov.sk/sekcie/informatizacia/kyberneticka-bezpecnost/bezpecnostnadokumentacia-metodiky/index.html">https://www.mirri.gov.sk/sekcie/informatizacia/kyberneticka-bezpecnost/bezpecnostnadokumentacia-metodiky/index.html</a>
D.2		Vytvoriť šablóny a vzory dokumentácie bezpečnosti informačných technológií verejnej správy, návrhov, 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	Zverejnenie uceleného dokumentu so šablónami a vzormi dokumentácie podľa požiadaviek vyhlášky č. 179/2020 Z. z.	Plní sa	Plnené priebežne. MIRRI SR na svojom webovom sídle priebežne zverejňuje a aktualizuje vzory dokumentácie pre implementáciu týchto opatrení. Súčasťou budú aj návody a školiace materiály. Predpokladaný termín dokončenia úlohy najneskôr do: 12/2024	<a href="https://www.mirri.gov.sk/sekcie/informatizacia/kyberneticka-bezpecnost/bezpecnostnadokumentacia-metodiky/index.html">https://www.mirri.gov.sk/sekcie/informatizacia/kyberneticka-bezpecnost/bezpecnostnadokumentacia-metodiky/index.html</a>
D.4		Vytvoriť metodiku riadenia kybernetickej bezpečnosti vo vzťahu s tretími stranami v oblasti zaistenia bezpečnosti pri dodávateľských službách	MIRRI SR		03/2022	Zverejnenie metodiky	Splnené	Metodika bola zverejnená na webovom sídle ministerstva	<a href="https://www.mirri.gov.sk/sekcie/informatizacia/kyberneticka-bezpecnost/bezpecnostnadokumentacia-metodiky-pre-minimalnebezpecnostne-opatrenia-kategorie-i/index.html">https://www.mirri.gov.sk/sekcie/informatizacia/kyberneticka-bezpecnost/bezpecnostnadokumentacia-metodiky-pre-minimalnebezpecnostne-opatrenia-kategorie-i/index.html</a>

Kybernetická bezpečnosť ako základná súčasť verejnej správy – tabuľka 1/2

Kód úlohy	Úloha	Popis úlohy	Zodpovedný subjekt	Súčinný subjekt	Časový horizont realizácie	Návrh merateľných ukazovateľov	Stav plnenia	Spôsob plnenia	Dôkaz
D.8	<b>Zabezpečovanie prevencie a riešenia závažných bezpečnostných incidentov vo verejnej správe prostredníctvom jednotky CSIRT.SK</b>	Vytvoriť centrálny katalóg hrozieb pre verejnú správu	MIRRI SR		12/2022	Vytvorený katalóg hrozieb pre verejnú správu	Nesplnené	Vytvorenie centrálného katalógu hrozieb pre verejnú správu je predpokladané v termíne najneskôr do 12/2024.	
D.10	<b>Zabezpečenie adekvátnych odborných kapacít verejnej správy</b>	Určiť schému nevyhnutných počtov obsadenia odbornými pozíciami v jednotlivých orgánoch verejnej správy a spôsobu ich naplnenia	MIRRI SR		03/2022	Vytvorená schéma nevyhnutných počtov odborných pozícií v orgánoch verejnej správy	Splnené	Schéma nevyhnutných počtov odborných pozícií u subjektov verejnej správy bola vypracovaná	V priebehu roka 2023 bude spustený nový centrálny webový portál, kde budú tieto dokumenty uverejnené v jednotnom formáte
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	Strategický dokument definujúci pracovné pozície a znalostné požiadavky	Splnené	Dokument definujúci pracovné pozície vo verejnej správe a znalostné požiadavky bol vypracovaný	V priebehu roka 2023 bude spustený nový centrálny webový portál, kde budú tieto dokumenty uverejnené v jednotnom formáte

# Silné partnerstvá

Kód úlohy	Úloha	Popis úlohy	Zodpovedný subjekt	Súčinný subjekt	Časový horizont realizácie	Návrh merateľných ukazovateľov	Stav plnenia	Spôsob plnenia	Dôkaz
E.1	<b>Aktívna participácia na medzinárodnej diskusii v oblastiach kybernetickej bezpečnosti a kybernetickej diplomacie a následná implementácia dohodnutých záväzkov</b>	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	Odpočet aktivít	Priebežne plnené	Aktívna účasť na HWPCI, aktívna účasť na pracovných skupinách pod NIS Cooperation Group a Komisiou.	Ročná správa o KB
E.2		Aktívne sa podieľať na implementácii Stratégie kybernetickej bezpečnosti EÚ	NBÚ	MZVEZ SR	priebežne	Odpočet aktivít	Priebežne plnené	NBÚ adekvátne implementuje Stratégiu KB EÚ vo svojich aktivitách	Ročná správa o KB
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	<ul style="list-style-type: none"> <li>Miera implementácie opatrení na budovanie dôvery, vytvorených v rámci OBSE (tzv. CBMs)</li> <li>Odpočet aktivít</li> </ul>	Priebežne plnené	Aktivity zástupcov SR v rámci medzinárodných organizácií a procesov zameraných na problematiku tvorby medzinárodných noriem správania sa štátov v kybernetickom priestore: EÚ – Horizontálna pracovná skupina pre kybernetické otázky, OSN – Otvorená pracovná skupina pre bezpečnosť a využívanie informačných technológií v kontexte medzinárodnej bezpečnosti (OEWG), OBSE – Neformálna pracovná skupina (IWG) pre otázky IKT	odpočet zaslaný predsedovi Monitorovacieho výboru

Silné partnerstvá – tabuľka 1/7

Kód úlohy	Úloha	Popis úlohy	Zodpovedný subjekt	Súčinný subjekt	Časový horizont realizácie	Návrh merateľných ukazovateľov	Stav plnenia	Spôsob plnenia	Dôkaz
E.4	<b>Aktívna participácia na medzinárodnej diskusii v oblastiach kybernetickej bezpečnosti a kybernetickej diplomacie a následná implementácia dohodnutých záväzkov</b>	Spolupracovať so spojencami pri implementácii politik a posilňovaní nástrojov NATO v oblasti kybernetickej obrany v kontexte kolektívnej obrany	NBÚ, MO SR	MZVEZ SR	priebežne	<ul style="list-style-type: none"> <li>Participácia na rokovaní príslušných výborov a pracovných skupín NATO; a</li> <li>Bilaterálna spolupráca s vybranými spojencami a partnerskými krajinami NATO v oblasti kybernetickej obrany</li> </ul>	Priebežne plnené	<p>Účast na stálej pracovnej skupine – Cyber Defense Committee (CDC) a iných odborných pracovných a riadiacich skupín NATO;</p> <p>Účast na projekte stálej štruktúrovanej spolupráce EÚ (PESCO) – Cyber and Information Domain Coordination Center (CIDCC) – 10/2022;</p> <p>Pristúpenie k projektu Európskej obrannej agentúry (EDA) – Military Computer Emergency Response Team Operational Network (MICNET) – 11/2022; Pravidelné bilaterálne rokovania s vybranými spojencami na území SR, ako aj v zahraničí.</p> <p>Oslovenie NBÚ rozšírenie prístupových práv VS k projektu smart defence NATO – MISP.</p>	<p>Závery rokovaní multilaterálnych a bilaterálnych rokovaní nie je možné zverejniť nakoľko ide o utajované skutočnosti v zmysle Zákona č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov.</p> <p>CIDCC: <a href="https://defence.hu/news/european-union-cyber-defence-consultation-in-budapest.html">https://defence.hu/news/european-union-cyber-defence-consultation-in-budapest.html</a></p> <p>MICNET: <a href="https://eda.europa.eu/news-and-events/news/2022/11/15/a-new-budget-for-a-new-era-eu-defence-ministers-approve-eda-budget-increase">https://eda.europa.eu/news-and-events/news/2022/11/15/a-new-budget-for-a-new-era-eu-defence-ministers-approve-eda-budget-increase</a></p>
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	Identifikovať a vstúpiť do vybraného projektu PESCO	Priebežne plnené	<p>V prvej polovici roka 2022 SR prostredníctvom VS pristúpila k projektu kybernetickej obrany PESCO – Cyber Information Domain Coordination Centre (CIDCC) v pozícii pozorovateľskej krajiny. V súčasnosti prebieha proces zmeny formy nášho členstva na riadne členstvo.</p>	<p>CIDCC – brožúra dostupná na: <a href="https://www.google.com/url?sa=t&amp;rct=j&amp;q=&amp;e-source=web&amp;cd=&amp;cad=rja&amp;uact=8&amp;ved=2ahUKEwjfoozsy4X9AhU6_rslHcX-FAR8QFnoECBUQAQ&amp;url=https%3A%2F%2Fwww.pesco.europa.eu%2Fp-content%2Fuploads%2F2022%2F10%2F-Flyer-CIDCC-221004.pdf&amp;usg=AOvVaw2wNnHsIR8y-Hc6y82yOnLQC">https://www.google.com/url?sa=t&amp;rct=j&amp;q=&amp;e-source=web&amp;cd=&amp;cad=rja&amp;uact=8&amp;ved=2ahUKEwjfoozsy4X9AhU6_rslHcX-FAR8QFnoECBUQAQ&amp;url=https%3A%2F%2Fwww.pesco.europa.eu%2Fp-content%2Fuploads%2F2022%2F10%2F-Flyer-CIDCC-221004.pdf&amp;usg=AOvVaw2wNnHsIR8y-Hc6y82yOnLQC</a></p>



Kód úlohy	Úloha	Popis úlohy	Zodpovedný subjekt	Súčinný subjekt	Časový horizont realizácie	Návrh merateľných ukazovateľov	Stav plnenia	Spôsob plnenia	Dôkaz
E.6	<b>Aktívne pôsobenie v medzinárodnom prostredí zamerané na presadenie noriem zodpovedného správania sa v kybernetickom priestore</b>	Na pôde OSN sa zasadzovať za pokračovanie úsilia zameraného na posilnenie noriem, princípov a pravidiel používania IKT s cieľom zaviazat štáty k zodpovednému správaniu v kybernetickom priestore, uplatňovať medzinárodné právo a budovať dôveru s cieľom prevencie nestability a posilňovania bezpečnosti	MZVEZ SR	NBÚ	priebežne	Odpočet aktivít	Priebežne plnené	Aktivity zástupcov SR v rámci procesov OSN zameraných na problematiku tvorby medzinárodných noriem správania sa štátov v kybernetickom priestore.	
E.7		Aktívne sa podieľať na tvorbe a implementácii kybernetických bezpečnostných 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	Odpočet aktivít	Priebežne plnené	Účast na rokovaniach OSCE, aktívna účasť pri komunikačných cvičeniach	Ročná správa o KB
E.8		V rámci členstva v medzinárodných organizáciách (RE, EÚ, OSN, OECD) presadzovať riešenia, ktoré prispievajú k efektívnejšiemu stíhaniu počítačovej kriminality pri zachovaní základných požiadaviek na ochranu základných práv a slobôd	MS SR	NBÚ, MZVEZ SR	priebežne		Neodpočítované		
E.9	<b>Nadväzovať a posilňovať bilaterálnu spoluprácu SR v oblasti kybernetickej bezpečnosti.</b>	Vytvárať a posilňovať partnerskú spoluprácu s vybranými štátmi v rámci kybernetickej bezpečnosti zameranú na rozširovanie spoluprác 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	Odpočet aktivít v zmysle iniciovania spolupráce	Priebežne plnené	Udržiavanie a rozvíjanie bilaterálnych vzťahov s partnerskými krajinami. Nadviazanie bilaterálnej spolupráce s Indonéziou (podpis memoranda začiatkom roka 2023)	Ročná správa o KB

Silné partnerstvá – tabuľka 3/7

Kód úlohy	Úloha	Popis úlohy	Zodpovedný subjekt	Súčinný subjekt	Časový horizont realizácie	Návrh merateľných ukazovateľov	Stav plnenia	Spôsob plnenia	Dôkaz
E.10	<b>Nadväzovať a posilňovať bilaterálnu spoluprácu SR v oblasti kybernetickej bezpečnosti</b>	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	Odpočet aktivít	Priebežne plnené	Aktívna účasť na konferenciách a aktivitách Trusted Introducer a FIRST, aktívna účasť v pracovných skupinách pre štandardizáciu FIRST	Ročná správa o KB
E.11	<b>Posilniť systémove pokrývanie agendy kybernetickej bezpečnosti a diplomacie na vybraných zastupiteľstvách SR v zahraničí a zo Slovenska</b>	V rámci existujúcich kapacít rozšíriť zameranie činnosti zastupiteľských úradov vo vybraných krajinách o problematiku kybernetickej bezpečnosti a diplomacie, vrátane rozširovania stykovej a spravodajskej činnosti v tejto oblasti	MZVEZ SR	NBÚ	priebežne	Odpočet aktivít	Priebežne plnené	<ul style="list-style-type: none"> <li>Na všetky ZÚ SR bol odoslaný inštrukčný list s pokynom priebežne sledovať, informovať a vyhodnocovať politiky a opatrenia krajín pôsobenia v oblasti kybernetickej bezpečnosti a aktívne nadväzovať a prehlbovať spoluprácu so spojencami a krajinami EÚ v tejto oblasti. ZÚ SR v krajinách EÚ a NATO boli inštruované aby sledovali a informovali o iniciatívach a postojoch krajiny akreditácie k prebiehajúcim procesom v agende hybridných hrozieb, vrátane opatrení na posilňovanie odolnosti voči dezinformáciám a kybernetickým útokom.</li> <li>Stále zastúpenia SR pri medzinárodných organizáciách boli inštruované, aby aktívne pokrývali agendu kybernetickej bezpečnosti v úzkej spolupráci s vecne príslušnými rezortami a inštitúciami pri vzájomnej koordinácii a zabezpečení efektívneho toku informácií. Vzhľadom aj na postupné rozšírenie kapacít v oblasti kybernetickej bezpečnosti a diplomacie na MZVEZ, sa zefektívnila spolupráca medzi relevantnými stálymi zastúpeniami a ústredím</li> </ul>	K dňu odpočtu plnenia úloh vyplývajúcich z Akčného plánu (ku koncu 2022) agenda kybernetickej bezpečnosti bola systémove zabezpečená na nasledujúcich zastupiteľských úradoch SR: <ul style="list-style-type: none"> <li>všetky stále zastúpenia SR pri medzinárodných organizáciách (5)</li> <li>16 zastupiteľských úradov (UK, FR, CZ, DE, KR, LV, CN, PL, FI, AU, HU, AT, RU, US, SE, TR)</li> <li>Je dôležité spomenúť, že sme zaznamenali zvýšený záujem zo strany EÚ o informácie týkajúce sa personálneho pokrytia/ zabezpečenia agendy kybernetickej bezpečnosti a diplomacie na zastupiteľských úradoch a stálych misiách SR.</li> </ul>

Kód úlohy	Úloha	Popis úlohy	Zodpovedný subjekt	Súčinný subjekt	Časový horizont realizácie	Návrh merateľných ukazovateľov	Stav plnenia	Spôsob plnenia	Dôkaz
E.12	<b>Posilniť systémove pokrývanie agendy kybernetickej bezpečnosti a diplomacie na vybraných zastupiteľstvách SR v zahraničí a zo Slovenska</b>	Pokračovať v rozvoji medzinárodnej spolupráce v agende kybernetickej bezpečnosti na vybraných zastupiteľských úradoch a z centra prostredníctvom pracovníkov NBÚ v pozícii kyberatašé a dosiahnuť pokrytie najmenej EÚ, Spojeného kráľovstva, Severnej Ameriky a Ázie	NBÚ	MZVEZ SR	6/2022	Počet kybernetických diplomatov	Plní sa	NBÚ momentálne pripravuje pokrytie ďalších zastúpení mimo EÚ	
E.13	<b>Podporovať zapájanie slovenských podnikov, mimovládnych organizácií, či akademickej sféry do medzinárodných aktivít a iniciatív v oblasti kybernetickej bezpečnosti</b>	Aktívne podporovať a vyhľadávať príležitosti pre zapájanie slovenských podnikov, mimovládnych organizácií a akademickeho sektora do medzinárodnej spolupráce v oblasti kybernetickej bezpečnosti, vrátane zdieľania ich expertízy a nadväzovania obchodnej spolupráce	MZVEZ, NBÚ	KCKKB	priebežne	<ul style="list-style-type: none"> <li>Zriadené štruktúry NCC, zverejnené výzvy</li> <li>Odpočet aktivít</li> <li>Objem finančných prostriedkov z priamo riadených programov pridelených slovenským subjektom v oblasti kybernetickej bezpečnosti</li> </ul>	Priebežne plnené	Na všetky ZÚ SR a stále zastúpenia pri medzinárodných organizáciách bola zaslaná inštrukcia sledovať a informovať o systémových opatreniach zameraných na prehľadovanie spolupráce vlád so súkromným sektorom v oblasti boja s dezinformáciami a kybernetickej bezpečnosti, ako aj riešenie výziev spojených s postupujúcou digitalizáciou a nástupom moderných technológií	Odpočet zaslaný predsedovi Monitorovacieho výboru
E.14	<b>SK-ISAC</b>	Pripraviť a implementovať model skupín pre spoluprácu v oblasti kybernetickej bezpečnosti na sektorovej úrovni (model ISAC)	NBÚ	PZS	12/2021	Vytvorenie modelu ISAC	Plní sa	Takáto platforma bude vytvorená v rámci pracovných skupín NCC	<a href="https://www.kyberkomunita.sk/pracovneskupiny/">https://www.kyberkomunita.sk/pracovneskupiny/</a>
E.15	<b>Národná CSIRT sieť</b>	Zriadiť národnú CSIRT sieť, ktorá bude združovať CSIRT jednotky z verejného, súkromného a akademickeho sektora	NBÚ	MIRRI SR	01/2022	Zriadenie národnej CSIRT siete	Plní sa	Národná CSIRT sieť bude vytvorená v rámci jednej z pracovných skupín NCC	<a href="https://www.kyberkomunita.sk/pracovneskupiny/">https://www.kyberkomunita.sk/pracovneskupiny/</a>

Silné partnerstvá – tabuľka 5/7

Kód úlohy	Úloha	Popis úlohy	Zodpovedný subjekt	Súčinný subjekt	Časový horizont realizácie	Návrh merateľných ukazovateľov	Stav plnenia	Spôsob plnenia	Dôkaz
E.17	<b>Spolupráca v oblasti kybernetickej obrany</b>	Posilňovať spoluprácu rezortu obrany s príslušnými štátnymi inštitúciami, súkromným sektorom a akademickou obcou na národnej aj medzinárodnej úrovni	MO SR		Priebežne	<ul style="list-style-type: none"> <li>Nastavovanie formalizovanej spolupráce;</li> <li>Poskytovanie odbornej asistencie; a</li> <li>Riešenie kybernetických bezpečnostných incidentov.</li> </ul>	Priebežne plnené	Rozšírenie počtu existujúcich dohôd o spolupráci v oblasti kybernetickej bezpečnosti a obrany s vybranými národnými partnermi pôsobiacimi na úseku obrany; Vykonávanie testovania zraniteľností na základe žiadosti; Riešenie kybernetických bezpečnostných incidentov v pôsobnosti rezortu obrany na základe žiadosti o poskytnutie súčinnosti (napr. kybernetický bezpečnostný incident III. stupňa); a Plnenie úloh stanovených Bezpečnostnou radou Slovenskej republiky v spolupráci s ostatnými bezpečnostnými a spravodajskými zložkami.	Správa o činnosti Vojenského spravodajstva za rok 2022
E.18	<b>Kolektívna obrana</b>	Urýchľovať implementáciu medzinárodných záväzkov SR v rámci kolektívnej obrany	MO SR	NBÚ	Priebežne	Implementácia platných a novo schválených politických a odborných záväzkov.	Priebežne plnené	Implementácia Spoločnej spojeneckej doktríny pre operácie v kybernetickom priestore/ Allied Joint Doctrine for cyber space operations (AJP 3.20); Plnenie existujúcich Cieľov spôsobilostí a participácia na príprave nových Cieľov spôsobilostí; Plnenie záväzkov Cyber Pledge at 28; a Participácia na činnosti Koordinovaného ročného prehľadu o obrane EÚ (CARD).	Správa o činnosti Vojenského spravodajstva za rok 2022

Kód úlohy	Úloha	Popis úlohy	Zodpovedný subjekt	Súčinný subjekt	Časový horizont realizácie	Návrh merateľných ukazovateľov	Stav plnenia	Spôsob plnenia	Dôkaz
E.19	<b>Pôsobenie v medzinárodnom prostredí zamerané na optimalizáciu noriem prijatých na pôde Medzinárodnej agentúry pre atómovú energiu (MAAE) pre zodpovedné správanie sa v kybernetickom priestore jadrových zariadení</b>	Pokračovať v rozvoji medzinárodnej spolupráce v agende kybernetickej bezpečnosti v expertných skupinách MAAE a prostredníctvom pracovníkov Úradu jadrového dozoru Slovenskej republiky (ÚJD SR)	ÚJD SR	MZVEZ SR, NBÚ	Priebežne	<ul style="list-style-type: none"> <li>Účast' na konferencii, technickom seminári, alebo školení aspoň 1 krát ročne organizovanom Medzinárodnou agentúrou pre atómovú energiu (MAAE) so sídlom vo Viedni</li> <li>Účast' na tvorbe, alebo aktualizácii medzinárodných noriem a technických dokumentácií v oblasti fyzickej bezpečnosti jadrových zariadení a ich kybernetickej bezpečnosti, v rámci pracovných skupín (MAAE) formou návrhov, pripomienok, prezentácií, alebo zdieľaním</li> <li>výsledkov</li> </ul>	Priebežne plnené	Účast' na webinároch, mítingoch a konferenciách	<p>Webinar on National Nuclear Security Threat Assessment, Design Basis Threats and Representative Threat Statements (Februar 2022) Meeting of Legal and Technical Experts on the Need for Revision of the Nuclear Security Fundamentals (NSS No. 20) (Januar 2022)</p> <p>Open-Ended Consultations in Advance of the 2022 Conference of the Parties to the A/CPPNM (22.3.2022, 21.3.2022, 17. - 18.3.2022, 1.3.2022, 28.2.2022, 17.2.2022, 2.2.2022, 24.1.2022)</p> <p>A/CPPNM Review Conference March (28.3 – 1.4.2022 RTC on Computer Security Fundamentals for Nuclear Security (31. 10. 2022- , 4. 11. 2022) Viena, Austrália)</p> <p>Účast' na mítingoch NSGC – NUCLEAR SECURITY GUIDANCE COMMITTEE, zaoberajúca sa tvorbou a revíziou dokumentov MAAE v oblasti fyzickej ochrany jadrových materiálov, jadrových zariadení a ich kybernetickej bezpečnosti. (13 – 16 jún 2022)</p>

Silné partnerstvá – tabuľka 7/7

## Vzdelaní odborníci a vzdelaná verejnosť

Kód úlohy	Úloha	Popis úlohy	Zodpovedný subjekt	Súčinný subjekt	Časový horizont realizácie	Návrh merateľných ukazovateľov	Stav plnenia	Spôsob plnenia	Dôkaz
F.2	<b>Východiská vzdelávania v oblasti kybernetickej bezpečnosti</b>	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	Počet ročníkov, pre ktoré sú požiadavky definované	Nesplnené		
F.3		Dopracovať aktuálne a vznikajúce zamestnania zaoberajúce sa kybernetickou bezpečnosťou do registra zamestnaní vrátane ich kompetenčných a kvalifikačných úrovní v rámci Národnej sústavy povolání v súlade s Národným kvalifikačným rámcom SR a Národnou sústavou kvalifikácií (odborné vedomosti, odborné zručnosti, všeobecné spôsobilosti)	MŠVVaŠ SR	MPSVaR SR, KCCKB, Aliancia sektorových rád, tretí sektor	03/2022	Identifikácia a dopracovanie (zoznam) zamestnaní (aktuálnych a vznikajúcich) zaoberajúcich sa kybernetickou bezpečnosťou, ktoré nie sú dopracované do registra zamestnaní (ich kompetenčné úrovne, a kvalifikačné úrovne)	Splnené	Slovenský kvalifikačný rámec (SKKR) je nástroj, ktorý na základe vopred stanovených kritérií priraduje určitú úroveň jednotlivým kvalifikáciám z Národnej sústavy kvalifikácií. Národné kvalifikácie a rôzne cesty ich získavania (formálne a neformálne vzdelávanie, informálne učenie sa) sa vďaka nemu stávajú zrozumiteľnejšie, porovnateľnejšie, prehľadnejšie a transparentnejšie. Slovenský kvalifikačný rámec má osem úrovní. Špecialista informačnej bezpečnosti <a href="https://www.kvalifikacie.sk/kartakvalifikacie/1387">https://www.kvalifikacie.sk/kartakvalifikacie/1387</a> Kód kvalifikácie U2529001-01387 Úroveň SKKR 6 <a href="https://www.kvalifikacie.sk/download-pdfkarta-kvalifikacie/1387">https://www.kvalifikacie.sk/download-pdfkarta-kvalifikacie/1387</a>	<a href="https://www.kvalifikacie.sk/katalog-skk">https://www.kvalifikacie.sk/katalog-skk</a>

Kód úlohy	Úloha	Popis úlohy	Zodpovedný subjekt	Súčinný subjekt	Časový horizont realizácie	Návrh merateľných ukazovateľov	Stav plnenia	Spôsob plnenia	Dôkaz
F.4	<b>Východiská vzdelávania v oblasti kybernetickej bezpečnosti</b>	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	revízia a dopracovanie profesijných štandardov	Plní sa	Čiastočne splnené. Aktualizované profesijné štandardy sú v procese interného schvaľovania a mali by byť zverejnené do konca roka 2022	Aktualizované profesijné štandardy budú zverejnené na stránke MŠVVaŠ
F.5		Dopracovať aktuálne a vznikajúce zamestnania zaoberajúce sa kybernetickou bezpečnosťou do registra zamestnaní vrátane ich kompetenčných a kvalifikačných úrovní v rámci Národnej sústavy povolání v súlade s Národným kvalifikačným rámcom SR a Národnou sústavou kvalifikácií (odborné vedomosti, odborné zručnosti, všeobecné spôsobilosti)	MŠVVaŠ SR	MPSVaR SR, KCCKB, Aliancia sektorových rád, tretí sektor	03/2022	revízia a dopracovanie profesijných štandardov	Plní sa	Čiastočne splnené. Aktualizované profesijné štandardy sú v procese interného schvaľovania a mali by byť zverejnené do konca roka 2022	Aktualizované profesijné štandardy budú zverejnené na stránke MŠVVaŠ
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	06/2022	Vypracovanie jednotnej metricky a vytvorenie dostupného testovacieho nástroja	Nesplnené	Vypracovanie jednotnej metricky a vytvorenie dostupného testovacieho nástroja	
F.7	<b>Budovanie základného povedomia a vzdelávanie v kybernetickej bezpečnosti v regionálnom školstve</b>	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	Zrealizovanie merania na štatisticky výpočtovej vzorke subjektov	Nesplnené		

Vzdelaní odborníci a vzdelaná verejnosť – tabuľka 2/11

Kód úlohy	Úloha	Popis úlohy	Zodpovedný subjekt	Súčinný subjekt	Časový horizont realizácie	Návrh merateľných ukazovateľov	Stav plnenia	Spôsob plnenia	Dôkaz
F. 8	<b>Budovanie základného povedomia a vzdelávanie v kybernetickej bezpečnosti v regionálnom školstve</b>	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	Zrealizovanie merania na štatisticky výpovednej vzorke subjektov	Nesplnené		
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	Pravidelné opakovanie meraní a ich vyhodnocovanie	Nesplnené		
F. 10		Navrhnuť 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	Vytvorenie metodiky, škálovanej podľa veku dieťaťa	Nesplnené		
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	Vypracovanie prehľadu o rizikách v súvislosti s interakciou detí a mládeže s IKT a internetom, jeho každoročná aktualizácia a diseminácia príslušným subjektom (napr. prostredníctvom regionálnych školských úradov, poradenských centier...na školy, do školských zariadení). Publikovaný zoznam rizík, ročne	Nesplnené		



Kód úlohy	Úloha	Popis úlohy	Zodpovedný subjekt	Súčinný subjekt	Časový horizont realizácie	Návrh merateľných ukazovateľov	Stav plnenia	Spôsob plnenia	Dôkaz
F. 13	<b>Budovanie základného povedomia a vzdelávanie v kybernetickej bezpečnosti v regionálnom školstve</b>	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	Pripraviť plán a implementovať ho na základe plánu obnovy pre regionálne školstvo vzdelávací štandard pre schopnosť logického myslenia, kritického myslenia, etiky a nevyhnutných digitálnych zručností v oblasti kybernetickej bezpečnosti	Neodpočítavané		
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 využitia na lokálnej a regionálnej úrovni	MŠVVaŠ SR	zriaďovatelia škôl, mestá a samosprávy kraje	priebežne	Pripraviť odporúčanie bezpečného používania IKT prostriedkov počas výučby a bezpečného vyučovania v online priestore	Neodpočítavané		
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	Počet vypracovaných metodík, cvičebníc a iných podkladov	Nesplnené		

Vzdelaní odborníci a vzdelaná verejnosť – tabuľka 4/11

Kód úlohy	Úloha	Popis úlohy	Zodpovedný subjekt	Súčinný subjekt	Časový horizont realizácie	Návrh merateľných ukazovateľov	Stav plnenia	Spôsob plnenia	Dôkaz
F. 24	<b>Budovanie základného povedomia a vzdelávanie v kybernetickej bezpečnosti v regionálnom školstve</b>	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	Počet multidisciplinárnych stretnutí zameraných na zlepšenie kvality bezpečnosti detí v online priestore	Priebežne plnené	<ul style="list-style-type: none"> <li>Počet zasadnutí pracovnej skupiny expertov: 2</li> <li>Organizácia konferencie „Bezpečnosť detí v digitálnom priestore“</li> <li>Aktivity v rámci plnenia Akčného plánu Národnej koncepcie ochrany detí v digitálnom priestore: 46 aktivít v rámci okresov Slovenskej republiky</li> </ul>	
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	Počet vytvorených grantových schém.	Nesplnené		
F. 26	<b>Vzdelávanie a príprava kvalitných IT špecialistov na kybernetickú bezpečnosť</b>	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	Vytvoriť koncept podpory odborného vzdelávania v oblasti kybernetickej bezpečnosti	Nesplnené		
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	Metodická podpora tvorby školských vzdelávacích programov v zmysle cieľa uvedenej úlohy – odpočet aktivít	Nesplnené		

Kód úlohy	Úloha	Popis úlohy	Zodpovedný subjekt	Súčinný subjekt	Časový horizont realizácie	Návrh merateľných ukazovateľov	Stav plnenia	Spôsob plnenia	Dôkaz
F. 29	<b>Vzdelávanie a príprava kvalitných IT špecialistov na kybernetickú bezpečnosť</b>	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	Revízia kategórií odborov na stredných školách a zýšenie normatívu	Nesplnené		
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		Neodpočítavané		
F. 33		Vytvoriť a akreditovať vysokoškolské študijné odbory v oblasti kybernetickej bezpečnosti	MŠVVaŠ SR	Vysoké školy	08/2022	Vytvorené a akreditované študijné odbory (poznámka – študijné odbory sa neakreditujú)	Nesplnené	Nesplnené. Študijné odbory sú dané vyhláškou č. 244/2019 Z. z. o sústave študijných odborov SR a nepodliehajú akreditácií. Opatrenie preto nie je možné vykonať. Ak boli opatrením myslené študijné programy, platí, že vysoké školy momentálne môžu požiadať o akreditáciu nových študijných programov len v študijných odboroch a stupňoch štúdiá, v ktorých ešte neuskutočňujú študijné programy. V prípade, že vysoká škola už uskutočňuje v študijnom odbore kybernetika alebo informatika študijný program, nemôže podľa § 36 ods. 1 zákona č. 269/2018 Z. z. o zabezpečovaní kvality vysokoškolského vzdelávania a o zmene a doplnení zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov požiadať v príslušnom stupni o akreditáciu nového študijného programu až pokiaľ nebude mať pozitívne posúdený vnútorný systém zabezpečovania kvality (predpokladá sa koniec roka 2023 alebo začiatok 2024). Akreditácia nových študijných programov v oblasti kybernetiky je teda možná v súčasnej dobe len v rámci vysokých škôl, ktoré ešte v danom	

Vzdelaní odborníci a vzdelaná verejnosť – tabuľka 6/11

Kód úlohy	Úloha	Popis úlohy	Zodpovedný subjekt	Súčinný subjekt	Časový horizont realizácie	Návrh merateľných ukazovateľov	Stav plnenia	Spôsob plnenia	Dôkaz
F. 35	<b>Vzdelávanie a príprava kvalitných IT špecialistov na kybernetickú bezpečnosť</b>	Vytvoriť koncepciu vzdelávania kybernetickej bezpečnosti na všetkých typoch vysokých škôl	MŠVVaŠ SR	Vysoké školy	12/2022	Vytvorená koncepcia	Nesplnené		
F. 36		V rámci relevantných a existujúcich vysokoškolských študijných odborov vytvoriť a akreditovať študijné predmety v oblasti kybernetickej bezpečnosti	Fakulty relevantných vysokých škôl	MPSVaR SR, zamestnávateľské zväzy, Rada zamestnávateľov pre OVP, samosprávne kraje	12/2021		Nesplnené		
F. 37		Posilniť popularizáciu stredoškolského i vysokoškolského štúdia technických a prírodovedných odborov (STEM) a kybernetickej bezpečnosti	MŠVVaŠ SR		12/2022	Počet grantových schém a popularizačných aktivít	Plní sa	Národný projekt IT Akadémie pod gesciou CVTI SR mal viacero podaktivít propagujúcich technické a prírodovedné odbory, ako aj kybernetickú bezpečnosť. Celý rozsah realizovaných aktivít sa nachádza na adrese <a href="https://itakademia.sk/">https://itakademia.sk/</a>	
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, zamestnávateľské zväzy, Rada zamestnávateľov pre OVP, samosprávne kraje	12/2022	Podpora regionálnych nadpodnikových centier – odpočet aktivít Počet nadpodnikových centier, ktoré sa venujú kybernetickej bezpečnosti	Nesplnené		

Kód úlohy	Úloha	Popis úlohy	Zodpovedný subjekt	Súčinný subjekt	Časový horizont realizácie	Návrh merateľných ukazovateľov	Stav plnenia	Spôsob plnenia	Dôkaz
F.39	<b>Vzdelávanie a zvyšovanie bezpečnostného povedomia zamestnancov verejnej správy - bezpečnostného povedomia zamestnancov verejnej správy</b>	Vytvoriť plán financovania, prijímania, udržania, zabezpečenia a kariérneho rastu zamestnancov verejnej správy	MIRRI SR	Akademický sektor, KCC-KB, MŠVVaŠ SR, SIS	12/2022	Vytvorenie programu vzdelávania	Nesplnené	Vytvorenie plánu je predpokladané v termíne najneskôr do 12/2024.	Program sa skladá z nasledujúcich častí: <ul style="list-style-type: none"> <li>• Reforma č. 5 Skvalitnenie vzdelávania a zabezpečenie spôsobilostí v oblasti kybernetickej a informačnej bezpečnosti (KIB) (ITVS), Komponent 17, Plán obnovy a odolnosti SR. Dostupné na: <a href="http://www.planobnovy.sk">www.planobnovy.sk</a> Výzva pre kompetenčné centrá bude zverejnená až v Q2-Q3/2023.</li> <li>• Národný projekt Výcvikové a školiace stredisko pre bezpečnosť prevádzky a správy IT pre sektor VS, Kód MetaIS: projekt_1450</li> </ul>
F.40		Vytvoriť plán financovania, prijímania, udržania, zabezpečenia a kariérneho rastu zamestnancov verejnej správy	MIRRI SR		12/2022	Vytvorený plán	Nesplnené	Vytvorenie plánu je predpokladané v termíne najneskôr do 12/2024.	
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	<ul style="list-style-type: none"> <li>• Počet zrealizovaných odborných školení; a</li> <li>• Účasť na odborných školeniach 3. strán doma i v zahraničí.</li> </ul>	Splnené	Boli vykonávané školenia pre civilný a vojenský personál pôsobiaci v SR, ako aj na zahraničných pracoviskách.	Správa o činnosti Vojenského spravodajstva za rok 2022

Vzdelaní odborníci a vzdelaná verejnosť – tabuľka 8/11

Kód úlohy	Úloha	Popis úlohy	Zodpovedný subjekt	Súčinný subjekt	Časový horizont realizácie	Návrh merateľných ukazovateľov	Stav plnenia	Spôsob plnenia	Dôkaz
F.45	<b>Vzdelávanie a zvyšovanie bezpečnostného povedomia zamestnancov verejnej správy- bezpečnostného povedomia zamestnancov verejnej správy</b>	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	<ul style="list-style-type: none"> <li>Účast' na cvičeniach kybernetickej obrany doma i v hraničích; a</li> <li>Inkorporovanie kybernetickej domény do národných vojenských cvičení.</li> </ul>	Priebežne plnené	V hodnotenom období rezort obrany participoval na všetkých dostupných cvičeniach kybernetickej obrany a kybernetickej bezpečnosti NATO a EÚ; a V rámci národných vojenských cvičení rezort obrany pravidelne inkorporoval kybernetický aspekt	Účast' VS na cvičení kybernetickej obrany: NATO Locked Shields 2022 – <a href="https://ccdcoe.org/exercises/locked-shields/">https://ccdcoe.org/exercises/locked-shields/</a> NATO Cyber Coalition 2022 – <a href="https://act.nato.int/articles/exercise-cyber-coalition-2022-concludes-estonia-Crossed-Swords-2022">https://act.nato.int/articles/exercise-cyber-coalition-2022-concludes-estonia-Crossed-Swords-2022</a> – <a href="https://ccdcoe.org/news/2022/exercise-crossedswords-2022-kicks-off/MIC22">https://ccdcoe.org/news/2022/exercise-crossedswords-2022-kicks-off/MIC22</a> – <a href="https://eda.europa.eu/news-and-events/news/2022/01/26/second-eda-live-cyberexercise-for-military-certs-concluded">https://eda.europa.eu/news-and-events/news/2022/01/26/second-eda-live-cyberexercise-for-military-certs-concluded</a>
F.48	<b>Vzdelávanie seniorov a ohrozených skupín</b>	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	Počet preventívnych aktivít zameraných na zvyšovanie povedomia znevýhodnených skupín o kybernetickej bezpečnosti	Plní sa	MV SR (OPK KMV SR) sa v rámci osvetovej činnosti venovalo aj zvyšovaniu povedomia rodičov a pestúnov detí o možných nebezpečenstvách v online prostredí. Činil tak prostredníctvom elektronických brožúr obsahujúcich praktické rady ako zabezpečiť účet na sociálnej sieti, či zamedziť zobrazovanie nevhodnému obsahu maloletým užívateľom. Samostatnú cieľovú skupinu tvorili seniori a to najmä z dôvodu zvýšeného počtu podvodných konaní páchaných práve na tejto cieľovej skupine. V roku 2021 bolo zrealizovaných 12 besied s 333 účastníkmi, ktoré boli zamerané na predchádzanie trestnej činnosti na senioroch vo fyzickom živote, ale aj v online prostredí. Ďalej bol strešným seniorským organizáciám pravidelne zasielaný krátky prehľad aktuálne páchaných podvodov na senioroch na Slovensku s krátkymi odporúčaniami slúžiacimi ako preventívna pomôcka. Záber tém komunikovaný týmto organizáciám je pomerne široký. Za relevantné príklady možno uviesť témy: overovanie osobných údajov cez telefón, nákupy online a internetové podvody, internetová peňaženka PayPal, nákupy v hrách – nástrahy mikrotransakcií, či narušenie (nabúranie) konta	

Kód úlohy	Úloha	Popis úlohy	Zodpovedný subjekt	Súčinný subjekt	Časový horizont realizácie	Návrh merateľných ukazovateľov	Stav plnenia	Spôsob plnenia	Dôkaz
F.49	<b>Koncept zvyšovania bezpečnostného povedomia</b>	Vytvoriť plán šírenia bezpečnostného povedomia v oblasti kybernetickej bezpečnosti	NBÚ		12/2021	Vytvorenie Národnej koncepcie šírenia bezpečnostného povedomia	Plní sa	NBÚ pripravuje koncepciu pre šírenie bezpečnostného povedomia	
F.50	<b>Kampane zvyšovania povedomia</b>	Organizovať a viesť kampane na zvyšovanie povedomia v oblasti kybernetickej bezpečnosti	NBÚ	sektorové ústredné orgány	priebežne	Odpočet aktivít	Priebežne plnené	Uverejňovanie článkov na webe SKCERT Spustenie kyberbezpečnostnej hry CyberGame Konferencie a workshopy pre verejnosť	www.sk-cert.sk
F.53	<b>Projekty a programy v oblasti vzdelávania a šírenia bezpečnostného povedomia</b>	Vytvoriť projekty na tvorbu open source programov v danej oblasti vzdelávania a šírenia situačného povedomia	KCCKB	NBÚ	06/2022	Publikovaná výzva	Priebežne plnené		

Vzdelaní odborníci a vzdelaná verejnosť – tabuľka 10/11

Kód úlohy	Úloha	Popis úlohy	Zodpovedný subjekt	Súčinný subjekt	Časový horizont realizácie	Návrh merateľných ukazovateľov	Stav plnenia	Spôsob plnenia	Dôkaz
F.55	<b>Vzdelávanie diplomatov</b>	Zaviest 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	Počet vyškolených vysielaných pracovníkov a zamestnancov z MZVEZ SR a ďalších rezortov (minimálne 50/rok)	<b>Priebežne plnené</b>	V rámci atestačného vzdelávania zamestnancov MZVEZ a prípravy na vyslanie do zahraničia a zamestnancov MZVEZ a pracovníkov ďalších rezortov vysielaných na zastupiteľské úrady v zahraničí bol zavedený a rozšírený prednáškový modul zameraný na kybernetickú bezpečnosť a diplomaciu. Vzdelávanie bolo zamerané na nasledujúce okruhy tém: <ul style="list-style-type: none"> <li>• hybridné hrozby a kybernetická bezpečnosť v kontexte medzinárodných vzťahov a medzinárodnej bezpečnosti (vývoj, trendy, perspektíva) -agenda kybernetickej bezpečnosti na pôde medzinárodných organizácií -inštitucionálne procesy v oblasti boja s hybridnými hrozbami a posilňovania odolnosti v podmienkach SR</li> <li>• kybernetické útoky/incidenty</li> <li>• Medzinárodná spolupráca v oblasti</li> <li>• posilňovania odolnosti voči kybernetickým útokom</li> <li>• Národné inštitúcie a legislatíva v oblasti kybernetickej bezpečnosti</li> </ul>	V roku 2022 odborné prednášky v oblasti kybernetickej bezpečnosti a diplomacie absolvovalo celkom 124 zamestnancov MZVEZ a pracovníkov iných rezortov vysielaných na ZÚ v zahraničí a to v rámci prípravy na vyslanie alebo v rámci atestačného vzdelávania



# Výskum a vývoj v oblasti kybernetickej bezpečnosti

Kód úlohy	Úloha	Popis úlohy	Zodpovedný subjekt	Súčinný subjekt	Časový horizont realizácie	Návrh merateľných ukazovateľov	Stav plnenia	Spôsob plnenia	Dôkaz
G.3	<b>Budovať odborné kapacity bezpečnostných tímov vrátane ich odborného vzdelávania</b>	Vytvoriť odborné pozície na vysokých školách za účelom prevádzky bezpečnostných systémov pre zber údajov a riešenie bezpečnostných incidentov	Vysoké školy	SAV, súkromný sektor	12/2021	Počet otvorených pozícií	Neodpočítané		
G.4	<b>Výskum v oblasti kybernetickej bezpečnosti pomocou metód umelej inteligencie</b>	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	Počet otvorených pozícií	Neodpočítané		
G.5	<b>Vytvorenie konzorcia pre výskum v oblasti kybernetickej bezpečnosti</b>	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	Zahájená štandardná činnosť pracovnej skupiny NCC „Výskum a vývoj“	Plní sa	Úlohu konzorcia bude plniť jedna z pracovných skupín NCC (Veda, výskum, inovácie)	<a href="https://www.kyberkomunita.sk/pracovneskupiny/">https://www.kyberkomunita.sk/pracovneskupiny/</a>
G.6	<b>Zmapovať súčasný stav vedy a výskumu v oblasti kybernetickej bezpečnosti na Slovensku</b>	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	Analýza súčasného stavu vedy a výskumu v oblasti kybernetickej bezpečnosti na Slovensku	Neodpočítané		

Výskum a vývoj v oblasti kybernetickej bezpečnosti – tabuľka 1/3

Kód úlohy	Úloha	Popis úlohy	Zodpovedný subjekt	Súčinný subjekt	Časový horizont realizácie	Návrh merateľných ukazovateľov	Stav plnenia	Spôsob plnenia	Dôkaz
G. 7	<b>Definovanie tém výskumu v oblasti kybernetickej bezpečnosti</b>	Vytvoriť úvodný zoznam výskumných tém v oblasti kybernetickej bezpečnosti a ich pravidelná aktualizácia (minimálne raz ročne)	Konzorcium		02/2022 a následne raz ročne		Neodpočítané	Naviazané na vznik konzorcia	
G. 9	<b>Zdieľanie dát pre výskumné účely</b>	Vytvoriť systém a podmienky pre zdieľanie dát pre výskumné účely za účelom tréningu a testovania neurónových sietí, pre metódy strojového učenia a iné výskumné účely	Konzorcium	Vysoké školy, SAV, NBÚ, MIRRI SR, súkromný sektor	06/2022		Neodpočítané	Naviazané na vznik konzorcia	
G. 11	<b>Podpora projektov v kybernetickej bezpečnosti v rámci plnenia úlohy národného koordinačného centra ECC</b>	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	Počet realizovaných projektov	Nesplnené		
G. 12	<b>Publikačná činnosť v kybernetickej bezpečnosti</b>	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	<ul style="list-style-type: none"> <li>Počet vedeckých prác publikovaných v recenzovaných periodikách</li> <li>Počet iných zverejnených publikácií</li> </ul>	Priebežne plnené	KCCKB pravidelne vydáva publikácie v KB. Na rok 2023 je pripravená aj výzva na grantové financovanie edície publikácií na rôzne témy súvisiace s KB	<a href="https://cybercompetence.sk/letaky/">https://cybercompetence.sk/letaky/</a>

Kód úlohy	Úloha	Popis úlohy	Zodpovedný subjekt	Súčinný subjekt	Časový horizont realizácie	Návrh merateľných ukazovateľov	Stav plnenia	Spôsob plnenia	Dôkaz
G. 13	<b>Technická normalizácia v kybernetickej bezpečnosti</b>	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	Zverejnený plán normalizačnej činnosti ÚNMS	Priebežne plnené	<ul style="list-style-type: none"> <li>• Preložená a prevzatá je norma STN ISO/IEC 27032. Pred dokončením je STN ISO/IEC 27037.</li> <li>• Pripravuje sa STN ISO/IEC 27001, STN ISO/IEC 27002, STN ISO/IEC 27005, , STN ISO/IEC 27013</li> </ul>	
G. 14	<b>Vytvorenie grantovej agentúry</b>	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	Zriadené štruktúry NCC, zverejnené výzvy	Nesplnené		
G. 15	<b>Poskytovanie grantových schém</b>	Poskytovať grantové schémy pre výskumné centrá na vysokých školách v oblasti kybernetickej bezpečnosti	KCCKB	MŠVVaŠ SR, Vysoké školy	priebežne	Zriadené štruktúry NCC, zverejnené výzvy	Nesplnené		
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	Zriadené štruktúry NCC, zverejnené výzvy	Nesplnené		

Výskum a vývoj v oblasti kybernetickej bezpečnosti – tabuľka 3/3





