Akčný plán realizácie Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020

Obsah

1

Úvod

Kybernetická bezpečnosť, ktorej cieľom je ochrana kybernetického priestoru, je neoddeliteľnou súčasťou bezpečnostného systému. **Kybernetický priestor** ponúka štátnym aktérom ponúka nové možnosti, ale zároveň **je zdrojom nových hrozieb** pre národnú a medzinárodnú bezpečnosť. Význam kybernetickej bezpečnosti je zdôraznený v strategických dokumentoch Organizácie Severoatlantickej zmluvy (ďalej len „NATO“) a Európskej únie (ďalej len „EÚ“), v ktorých sa potenciál kybernetických útokov definuje ako jedna z kľúčových hrozieb súčasného bezpečnostného prostredia. Z tohto dôvodu NATO pristúpilo **v rámci zabezpečenia kolektívnej obrany** k programu budovania a posilňovania kybernetických spôsobilostí s cieľom predchádzať, zaznamenávať, brániť sa a zotavovať sa z prípadných kybernetických útokov a EÚ definovala východiská a ciele kybernetickej bezpečnosti v podobe Stratégie kybernetickej bezpečnosti Európskej únie.

Budovanie národných kybernetických spôsobilostí bolo charakterizované intenzívnymi aktivitami v oblasti prípravy, tvorby a predkladania strategických a koncepčných materiálov pre oblasť kybernetickej bezpečnosti v SR. Tieto aktivity vyvrcholili prijatím **Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020** (ďalej len „Koncepcia“), ktorá bola schválená uznesením vlády SR č. 328 zo 17. Júna 2015 (ďalej len „uznesenie“).

Uznesením bola riaditeľovi Národného bezpečnostného úradu uložená úloha B.3. pripraviť a predložiť na rokovanie vlády SR návrh **Akčného plánu realizácie Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020** (ďalej len „Akčný plán“).

Z dôvodu urgentnosti a efektívnosti bol celý proces plnenia úloh na roky 2015-2020 vyplývajúcich z Koncepcie rozdelený na dve etapy v časovom horizonte plnenia v roku 2015 a v rokoch 2016-2020. Vybrané kľúčové úlohy dlhodobého charakteru v rámci oblasti inštitucionálneho rámca boli premietnuté v roku 2015 do plnenia úloh uložených uzneseniami vlády Slovenskej republiky, ako aj do novelizácií viacerých právnych predpisov nasledovne:

- prijatím zákona č. 339/2015 Z. z., ktorým sa mení a dopĺňa zákon č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov bola splnená úloha 1.1. z oblasti vytvorenia inštitucionálneho rámca riadenia kybernetickej bezpečnosti podľa Akčného plánu;

- zriadením Komisie pre kybernetickú bezpečnosť, ktorej štatút prerokovala vláda Slovenskej republiky a vzala na vedomie (č. m. UV-33740/2015), bola splnená úloha 1.2. z oblasti vytvorenia inštitucionálneho rámca riadenia kybernetickej bezpečnosti podľa Akčného plánu;

- prijatím zákona č. 346/2015 Z. z., ktorým sa mení a dopĺňa zákon č. 110/2004 Z. z o fungovaní Bezpečnostnej rady Slovenskej republiky v čase mieru v znení zákona č. 319/2012 Z. z., bola splnená úloha 1.7. z oblasti vytvorenia inštitucionálneho rámca riadenia kybernetickej bezpečnosti podľa Akčného plánu.

Plnenie úloh v druhej etape (2016-2020) je podrobne rozpracované v Akčnom pláne.

Gestorom Akčného plánu je **Národný bezpečnostný úrad ako ústredný orgán štátnej správy pre kybernetickú bezpečnosť** podľa § 34 zákona č. 575/2001 Z. z. o organizácii činnosti vlády a ústrednej štátnej správy v znení neskorších predpisov, pričom plnenie úloh uvedených v Akčnom pláne sa zveruje do zodpovednosti aj iným ministerstvám v rozsahu ich vecnej pôsobnosti a kompetencií.

Keďže strategickým cieľom kybernetickej bezpečnosti v Slovenskej republike je otvorený, bezpečný a chránený národný kybernetický priestor a vybudovanie dôvery v spoľahlivosť a bezpečnosť infraštruktúry, **koncepcia navrhla prijať a prioritne riešiť sedem opatrení:**

1) Vytvorenie inštitucionálneho rámca riadenia kybernetickej bezpečnosti.
2) Vytvorenie a prijatie legislatívneho rámca kybernetickej bezpečnosti.
3) Rozpracovanie a aplikácia základných mechanizmov zabezpečenia správy kybernetického priestoru.
4) Podpora, vypracovanie a zavedenie systému vzdelávania v oblasti kybernetickej bezpečnosti.
5) Stanovenie a aplikácia kultúry riadenia rizík a systému komunikácie medzi zainteresovanými stranami.
6) Aktívna medzinárodná spolupráca.
7) Podpora vedy a výskumu v oblasti kybernetickej bezpečnosti.

Jednotlivé úlohy sú obdobne ako v Koncepcii rozčlenené do siedmych strategických oblastí. V rámci jednotlivých oblastí Akčný plán **uvádza návrh úloh, spôsob ich realizácie, určuje zodpovedný orgán** (prípadne súčinnostný orgán), ako aj **časový rámec** (termín, príp. časové obdobie) ich **realizácie.** V každej oblasti sú úlohy rozpracované tak, aby napĺňali jednotlivé strategické ciele Koncepcie a tým dosiahli stav, kedy bude v Slovenskej republike ochrana národného kybernetického priestoru systémom fungujúcim **koncepčne, koordinovane, efektívne, účinne a na právnom základe** a bezpečnostné povedomie všetkých zložiek spoločnosti sa bude systematicky zvyšovať.

Návrh uvedených úloh si dáva taktiež za cieľ, **aby sa súkromný sektor, akademická obec, ako aj občianska spoločnosť aktívne zúčastňovala** na formovaní a realizácii politiky Slovenskej republiky

v oblasti kybernetickej bezpečnosti a aby bola zabezpečená **efektívna spolupráca na národnej, ako aj medzinárodnej úrovni.**

Treba zdôrazniť, že **navrhované úlohy a opatrenia na ich realizáciu sú adekvátne** a v primeranej miere rešpektujú ochranu súkromia občanov a základné ľudské práva a slobody. Práva, povinnosti ako aj úlohy jednotlivých aktérov v kybernetickom priestore budú stanovené v pripravovanom zákone o kybernetickej bezpečnosti.

Akčný plán bude aktualizovaný a priebežne vyhodnocovaný na základe výsledkov správy o stave kybernetickej bezpečnosti.

1. OBLASŤ: VYTVORENIE INŠTITUCIONÁLNEHO RÁMCA RIADENIA KYBERNETICKEJ BEZPEČNOSTI

Číslo úlohy	Úloha	Spôsob realizácie	Zodpovedný subjekt	Súčinnostný subjekt	Časový rámec realizácie
1.1.	Kompetenciu ústredného orgánu štátnej správy zveriť do pôsobnosti Národného bezpečnostného úradu	Zabezpečiť legislatívny proces novely kompetenčného zákona (zákona č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov) za účelom zverenia kompetencie ústredného orgánu štátnej správy pre kybernetickú bezpečnosť do pôsobnosti Národného bezpečnostného úradu	NBÚ	ÚV SR	12/2015
1.2.	Pripraviť návrh na vytvorenie formálnej platformy pre spoluprácu v oblasti kybernetickej bezpečnosti	Zriadiť Formálnu platformu pre spoluprácu verejnej správy, akademickej obce, vedeckých kruhov a súkromnej sféry vo forme Komisie pre kybernetickú bezpečnosť ako poradného orgánu riaditeľa Národného bezpečnostného úradu	NBÚ	ÚV SR	12/2015
1.3.	Zriadiť Národnú jednotku na riešenie incidentov	Navrhnúť organizačné, personálne, materiálno-technické a finančné zabezpečenie Národnej jednotky na riešenie incidentov	NBÚ	NASES	04/2016
		Určenie Národnej jednotky na riešenie incidentov	NBÚ	NASES	06/2016
		Dobudovanie vybraných spôsobilostí Národnej jednotky na riešenie incidentov	NBÚ	NASES	2018
1.4.	Predpoklady pre výkon kompetencií vecne príslušných autorít pre kybernetickú bezpečnosť	Navrhnúť personálne a materiálno-technické predpoklady pre výkon kompetencií vecne príslušných autorít pre kybernetickú bezpečnosť	ÚOŠS		04/2016
		Vytvoriť materiálno-technické zabezpečenie a konsolidáciu organizačného a personálneho zabezpečenia plnenia základných úloh vecne príslušných autorít	ÚOŠS		12/2017
		Zabezpečiť spoluprácu vecne príslušných autorít pre kybernetickú bezpečnosť	VPA		2016-2020

Číslo úlohy	Úloha	Spôsob realizácie	Zodpovedný subjekt	Súčinnostý subjekt	Časový rámec realizácie
1.5.	Dobudovať existujúce jednotky na riešenie incidentov	Dobudovať spôsobilosti a dosiahnuť plnú operačnú spôsobilosť CSIRT.MIL ako jednotky na riešenie incidentov pre účely obrany a bezpečnosti SR	MO SR		2016- 2018
		Dobudovať vybrané spôsobilosti CSIRT.SK – Vládnej jednotky na riešenie incidentov pri Datacentre (MF SR)	MF SR		2016-2020
1.6.	Budovať jednotky na riešenie bezpečnostných incidentov	Podľa požiadaviek zákona o kybernetickej bezpečnosti zabezpečiť výkon funkcionality jednotky na riešenie incidentov buď formou fyzického zriadenia pracoviska typu CERT/CSIRT v pôsobnosti vecne príslušných autorít alebo poveriť inú existujúcu jednotku na riešenie incidentov výkonom takejto funkcionality	VPA		2017-2020
1.7.	Zriadiť politickú úroveň rozhodovania v oblasti kybernetickej bezpečnosti	Zriadiť Výbor pre kybernetickú bezpečnosť ako poradný orgán Bezpečnostnej rady SR a organizačne stanoviť procesy jeho fungovania	ÚV SR	NBÚ	2016
1.8.	Vytvoriť rámec riadenia kybernetickej bezpečnosti v čase výnimočného stavu, vojnového stavu a vojny	Navrhnúť inštitucionálne riadenie kybernetickej bezpečnosti v núdzovom stave, výnimočnom stave, vojnovom stave a stave vojny	MO SR	NBÚ	12/207
		Navrhnúť kontingenčný plán prechodu zodpovednosti za riadenie kybernetickej bezpečnosti v čase mieru, núdzového stavu a výnimočného stavu do vojnového stavu a stavu vojny podľa ústavného zákona č. 227/2002 Z. z.	MO SR	NBÚ	12/2017
1.9.	Vytvoriť nadrezortný program „Ochrana kybernetického priestoru Slovenskej republiky“	V rámci priorít vlády SR predložiť na rokovanie vlády SR program „Ochrana kybernetického priestoru Slovenskej republiky“ v horizonte do roku 2025 obsahujúci súhrn projektov, aktivít, prác, činností a dodávok vykonávaných na splnenie zámerov a cieľov podľa rozpočtových pravidiel	NBÚ	MF SR ÚV SR	02/2016

2. OBLASŤ: VYTVORENIE A PRIJATIE LEGISLATÍVNEHO RÁMCA KYBERNETICKEJ BEZPEČNOSTI

Číslo úlohy	Úloha	Spôsob realizácie	Zodpovedný subjekt	Súčinnostný subjekt	Časový rámec realizácie
2.1.	Zabezpečiť schválenie legislatívneho zámeru zákona o kybernetickej bezpečnosti	Pripraviť návrh legislatívneho zámeru zákona o kybernetickej bezpečnosti	NBÚ		01/2016
		Zabezpečiť formálny legislatívny proces vo vzťahu k legislatívnemu zámeru zákona a kybernetickej bezpečnosti	NBÚ		03/2016
2.2.	Zabezpečiť prípravu, schválenie a implementáciu zákona o kybernetickej bezpečnosti	Pripraviť návrh zákona o kybernetickej bezpečnosti	NBÚ		06/2016
		Implementovať zákon o kybernetickej bezpečnosti do praxe	Ministerstvá a ÚOŠS		2017-2020
2.3.	Novelizovať súvisiace právne prepisy	Pripraviť návrh novelizácie súvisiacich predpisov, najmä: - zákon č. 45/2011 Z. z. o kritickej infraštruktúre za účelom spresnenia a rozšírenia definície sektorov kritickej infraštruktúry, ich gestorstva, ako aj prvkov kritickej infraštruktúry, zosúladenia so špecifikáciou obzvlášť dôležitých odvetví pre fungovanie vnútorného trhu podľa Návrhu Smernice Európskeho Parlamentu a Rady o opatreniach na zabezpečenie vysokej úrovne bezpečnosti sietí a informácií v Únii - Zákon č. 351/2011 Z.z. o elektronických komunikáciách za účelom stanovenia podmienok, za akých je operátor povinný uchovávať údaje o FO	NBÚ	MV SR MF SR MDVaRR	06/2016
2.4.	Pripraviť, schváliť a implementovať vykonávacie predpisy k zákonu o kybernetickej bezpečnosti	V nadväznosti na prijatie zákona o kybernetickej bezpečnosti pripraviť vykonávacie predpisy upravujúce podrobnosti oblastiam na základe blanketnej norme v zákone o kybernetickej bezpečnosti	NBÚ		12/2017
		Implementovať vykonávacie predpisy k zákonu o kybernetickej bezpečnosti do praxe	Ministerstvá a ÚOŠS		2018-2020
2.5.	Vydávať štandardy, metodiky a metodické usmernenia v oblasti kybernetickej bezpečnosti	V rámci Komisie pre kybernetickú bezpečnosť Národného bezpečnostného úradu zriadiť pracovnú skupinu pre metodiku a štandardy	NBÚ		03/2016

		V nadväznosti na prijatie zákona o kybernetickej bezpečnosti navrhnúť a prijať metodiky, štandardy a metodické usmernenia v oblastiach, ktoré ustanoví zákon o kybernetickej bezpečnosti	NBÚ		2017-2020
		Vytvoriť redakčný a publikačný systém pre štandardy a metodiku	NBÚ	NASES	09/2016
2.6.	Terminológia v oblasti kybernetickej bezpečnosti	Aktualizovať slovník krízového riadenia a doplniť ho o pojmy z oblasti kybernetickej bezpečnosti	BR SR		06/2016
		Pripraviť návrh terminologického výkladového slovníka kybernetickej bezpečnosti	NBÚ Akademická obec		2018

3. OBLASŤ: ROZPRACOVANIE A APLIKÁCIA ZÁKLADNÝCH MECHANIZMOV ZABEZPEČENIA SPRÁVY KYBERNETICKÉHO PRIESTORU

Číslo úlohy	Úloha	Spôsob realizácie	Zodpovedný subjekt		Časový rámec realizácie
3.1.	Vytvoriť národnú metodológiu na hodnotenie hrozieb a rizík v kybernetickom priestore	Navrhnúť a vytvoriť metodológiu hodnotenia rizík a hrozieb pre oblasť kybernetickej bezpečnosti na národnej úrovni	NBÚ		12/2016
		Uskutočniť hodnotenie rizík a hrozieb pre oblasť kybernetickej bezpečnosti na národnej úrovni podľa schválenej metodológie a následne pravidelne vyhodnocovať a aktualizovať riziká a hrozby pre oblasť kybernetickej bezpečnosti	NBÚ		2017
3.2.	V rámci mechanizmu prevencie zaviesť jednotné opatrenia z úrovne vecne príslušných autorít	Zaviesť opatrenia z úrovne vecne príslušných autorít, ktorých cieľom je pôsobiť proti vzniku krízových situácií a minimalizovať potenciálne riziká	VPA		2018
3.3.	Implementovať národnú politiku správania sa v kybernetickom priestore	Pripraviť, schváliť a implementovať do praxe politiku správania sa v kybernetickom priestore na národnej úrovni	NBÚ		2019
3.4.	Vytvoriť jednotný systém včasného varovania	Vytvoriť a implementovať jednotný systém včasného varovania, reakcie a výmeny informácií na zníženie rizík vyplývajúcich z hrozieb informačných a komunikačných systémov	NJRI	JRI	2016-2020
		Zriadiť Národný portál pre kybernetickú bezpečnosť ako súčasť ÚPVS	NBÚ	NASES	12/2016

3.5.	V rámci mechanizmu reakcie zaviesť na národnej úrovni jednotné opatrenia	Zaviesť jednotné opatrenia na národnej úrovni, ktorých cieľom bude kvalifikovane a efektívne reagovať v prípade bezpečnostného incidentu	NBÚ		2018
3.6.	Krízové plány riešenia krízových situácií pre oblasť kybernetickej bezpečnosti	Aktualizovať katalógové listy a doplniť ich tak, aby reflektovali bezpečnostné incidenty v rámci kybernetického priestoru	NBÚ		2017

4. OBLASŤ: PODPORA, VYPRACOVANIE A ZAVEDENIE SYSTÉMU VZDELÁVANIA V OBLASTI KYBERNETICKEJ BEZPEČNOSTI

Číslo úlohy	Úloha	Spôsob realizácie	Zodpovedný subjekt		Časový rámec realizácie
4.1.	Zmapovať súčasný stav vzdelávania v oblasti kybernetickej bezpečnosti	Zmapovať súčasný stav vzdelávania v oblasti kybernetickej bezpečnosti v rámci systémov: a) všeobecného vzdelávania (základný a stredný stupeň vzdelania) a b) odborného vzdelávania (stredný a vysokoškolský stupeň vzdelania, špecialisti)	MŠVVaŠ SR		06/2016
4.2.	Zabezpečiť vzdelávanie v oblasti kybernetickej bezpečnosti	Na základe výsledkov mapovania stavu vzdelávania spracovať návrh na inováciu a zabezpečenie vzdelávania v oblasti kybernetickej bezpečnosti v rámci systémov všeobecného vzdelávania (základný a stredný stupeň vzdelania) a podporu odborného vzdelávania (stredný a vysokoškolský stupeň vzdelania, špecialisti) v tejto oblasti	MŠVVaŠ SR	NBÚ NASES	03/2017
4.3.	Zaviesť inovovaný systém vzdelávania v oblasti kybernetickej bezpečnosti	Zaviesť inovovaný systém vzdelávania v oblasti kybernetickej bezpečnosti v rámci všeobecného vzdelávania (základný a stredný stupeň vzdelania) a podporiť odborné vzdelávanie (stredný a vysokoškolský stupeň vzdelania, špecialisti) v tejto oblasti	MŠVVaŠ SR		09/2018
4.4.	Vytvoriť Národné centrum vzdelávania v oblasti kybernetickej bezpečnosti	Vytvoriť Národné centrum vzdelávania v oblasti kybernetickej bezpečnosti, ktoré zabezpečí vzdelávanie a dosiahnutie aspoň základnej úrovne kompetencií v oblasti kybernetickej bezpečnosti všetkých pedagogických zamestnancov v regionálnom školstve, inovovať praktickú prípravu budúcich učiteľov	MŠVVaŠ SR	MF SR	06/2017

		jednotlivých stupňov škôl.			
4.5.	Systematicky zvyšovať povedomie o aspektoch kybernetickej bezpečnosti	Navrhnúť a zaviesť systematické šírenie osvety o bezpečnostných hrozbách, bezpečnostných rizikách a pravidlách správania sa v informačných systémoch verejnej správy	MF SR		06/2017
4.6.	Zabezpečiť školenia o kybernetickej bezpečnosti	V rámci rozvoja siete Govnet a služieb ÚPVS rozšíriť obsah existujúcich školení aj o kybernetickú bezpečnosť	NASES		2016-2020
		Rozšíriť existujúci projekt vzdelávania zamestnancov verejnej správy o oblasť kybernetickej bezpečnosti a zabezpečiť jeho realizáciu	MF SR		2017
Číslo úlohy	Úloha	Spôsob realizácie	Zodpovedný subjekt		Časový rámec realizácie
4.7.	Vytvoriť študijné programy v rámci celoživotného vzdelávania profesionálnych vojakov	V rámci Centra vzdelávania Akadémie ozbrojených síl vytvoriť programy pre všetkých profesionálnych vojakov so zameraním na kybernetickú bezpečnosť	MO SR		2017-2019
		V rámci Centra vzdelávania Akadémie ozbrojených síl vytvoriť programy pre všetkých profesionálnych vojakov – špecialistov IKT so zameraním na kybernetickú bezpečnosť	MO SR		2016-2017
4.8.	Zabezpečiť vzdelávanie v oblasti kybernetickej bezpečnosti v rámci justičných orgánov	Zaviesť minimálnu úroveň systematického vzdelávanie v oblasti kybernetickej bezpečnosti pre všetkých sudcov, prokurátorov a vyšetrovateľov na všetkých úrovniach	MS SR		2016-2020
		Zaviesť rozšírené vzdelávanie v oblasti kybernetickej bezpečnosti pre vybraných sudcov, prokurátorov a vyšetrovateľov na všetkých úrovniach	MS SR		2016-2020
4.9.	Šíriť osvetu v oblasti kybernetickej bezpečnosti	Spracovať návrh zabezpečenia systematického šírenia osvety v oblasti kybernetickej bezpečnosti	MK SR		2017

5. OBLASŤ: STANOVENIE A APLIKÁCIA KULTÚRY RIADENIA RIZÍK A SYSTÉMU KOMUNIKÁCIE MEDZI ZAINTERESOVANÝMI STRANAMI

Číslo úlohy	Úloha	Spôsob realizácie	Zodpovedný subjekt		Časový rámec realizácie
5.1.	Vytvoriť efektívny model spolupráce na národnej úrovni medzi jednotlivými subjektmi kybernetickej bezpečnosti .	Vytvoriť model spolupráce na národnej úrovni medzi pracoviskami typu CERT a CSIRT za účelom výmeny a zdieľania informácií najmä o bezpečnostných	NBÚ	JRI	2016

		incidentoch			
		Navrhnúť a vytvoriť bezpečný komunikačný kanál , prostredníctvom ktorého bude Národná jednotka na riešenie incidentov automatizovane prijímať štruktúrované správy s hláseniami o kybernetických bezpečnostných incidentoch na báze Govnetu	NJRI	NBÚ NASES	2017
		Vytvoriť efektívny model spolupráce na národnej úrovni medzi verejným sektorom, akademickou obcou a komerčnou sférou a vytvoriť platformu na ich spoluprácu.	NBÚ		2016-2020
5.2.	Stanoviť a implementovať systém nahlasovania a riešenia incidentov.	Implementovať on-line systém nahlasovania a riešenia incidentov.	NBÚ	NASES	2017

6. OBLASŤ: AKTÍVNA MEDZINÁRODNA SPOLUPRÁCA

Číslo úlohy	Úloha	Spôsob realizácie	Zodpovedný subjekt		Časový rámec realizácie
6.1.	V rámci členstva v EÚ sa aktívne zúčastňovať prípravy legislatívy a noriem týkajúcej sa kybernetickej bezpečnosti.	Zabezpečiť aktívnu účasť expertov predovšetkým na negociáciách k zneniu návrhu smernice o sieťovej a informačnej bezpečnosti	NBÚ	MZVaEZ	Priebežne
		Spolupracovať a aktívne sa podieľať na činnostiach a aktivitách medzinárodných platforiem v rámci medzinárodných organizácií v oblasti kybernetickej bezpečnosti.	NBÚ	MZVaEZ	2016-2020
		Počas predsedníctva SR v Rade EÚ zabezpečiť plnenie povinností SR súvisiacich s problematikou kybernetickej bezpečnosti.	MZVaEZ	NBÚ	07-12/2016
6.2.	V rámci členstva v NATO podporovať spoluprácu s NATO v oblasti kybernetickej obrany	Podpísať nové Memorandum o spolupráci v oblasti kybernetickej obrany	NBÚ	MO SR	01/2016
		Podporovať spoluprácu s NATO v oblasti kybernetickej obrany, najmä s ohľadom na reakcie na kybernetické bezpečnostné incidenty a výmenu technických informácií o hrozbách a zraniteľnostiach.	NBÚ	MO SR	2016-2020
6.3.	V rámci stredoeurópskeho priestoru rozvíjať spoluprácu	Aktívne sa podieľať , rozvíjať a podporovať spoluprácu v rámci krajín V4, predovšetkým prostredníctvom Stredoeurópskej platformy kybernetickej bezpečnosti (Central European Cyber Security Platform, CECSP)	NBÚ	MF SR MO SR NASES	Priebežne

6.4.	Zapájať sa a zúčastňovať sa na medzinárodných kybernetických cvičeniach	Pravidelne sa zúčastňovať a aktívne sa zapájať do medzinárodných kybernetických cvičení (Cyber Coalition, Locked Shields, Cyber Europe a iné)	NBÚ MF SR/DC MO SR		Priebežne
6.5.	Zintenzívniť spoluprácu s Centrom výnimočnosti pre kybernetickú obranu (NATO Cooperative Cyber Defence of Excellence – CCD CoE)	Navýšiť personálne kapacity zástupcov SR vyslaných na plnenie služobných povinností do CCD CoE	MO SR		2018

7. OBLASŤ: PODPORA VEDY A VÝSKUMU V OBLASTI KYBERNETICKEJ BEZPEČNOSTI

Číslo úlohy	Úloha	Spôsob realizácie	Zodpovedný subjekt		Časový rámec realizácie
7.1.	Podporovať výskumnú činnosť v oblasti kybernetickej bezpečnosti	Podporovať výskumnú činnosť v oblasti kybernetickej bezpečnosti prostredníctvom domácich grantových schém.	MŠVVaŠ SR		12/2020
		Podporovať výskumnú činnosť v oblasti kybernetickej bezpečnosti prostredníctvom prostriedkov vyčlenených pre Európsky výskumný priestor.	MŠVVaŠ SR		12/2020
7.2.	Podporovať budovanie forenzných pracovísk.	Koordinovať budovanie forenzných pracovísk za účelom výskumu potenciálnej zraniteľnosti systémov	NBÚ		2016-2020
		Budovať forenzné pracoviská zamerané na výkon analýz do vnútra organizácií.	ÚOŠS		2016-2020

Záver

Akčný plán stanovuje **cieľ zabezpečiť primeranú ochranu národného kybernetického priestoru** pred potenciálnymi a existujúcimi hrozbami, ktorých dôsledkom by mohli vzniknúť Slovenskej republike nenahraditeľné škody a mohla by byť narušená dôveryhodnosť štátu či organizácie. Koncepcia a Akčný plán, ako základné a východiskové dokumenty pre následnú tvorbu právnych predpisov, štandardov, metodických pokynov, pravidiel, bezpečnostných politík a iných nástrojov potrebných k zaisteniu ochrany a obrany národného kybernetického priestoru vytvárajú **predpoklady pre ucelený, koordinovaný a efektívny systém** ochrany kybernetického priestoru Slovenskej republiky.

Koncept návrhu úloh vychádzal zo strategických cieľov Koncepcie. Z dôvodu urgentnosti a efektívnosti boli niektoré z úloh bezodkladne premietnuté do plnenia úloh uznesení vlády Slovenskej republiky v roku 2015 (najmä uznesenie vlády Slovenskej republiky č. 328 zo dňa 17. júna 2015).

Akčný plán je navrhnutý na obdobie rokov 2015-2020. Predpokladané vplyvy realizácie Akčného plánu a ich **financovanie bude v roku 2016 pokryté v rámci schválených limitov** z bežných rozpočtových kapitol jednotlivých zodpovedných subjektov. **Národný bezpečnostný úrad v roku 2016 navrhne** vláde Slovenskej republike v rámci jej priorít **schváliť časovo neohraničený nadrezortný rozpočtový program „kybernetická bezpečnosť“** obsahujúci súhrn aktivít, prác, činností a dodávok vykonávaných na splnenie zámerov a cieľov podľa zákona o rozpočtových pravidlách vlády Slovenskej republiky, z ktorého bude finančne pokryté plnenie úloh, ktorých časový rámec realizácie je v rokoch 2017-2020.

V rámci zabezpečenia komplexnej kybernetickej bezpečnosti v spoločnosti, najmä na vytvorenie nástrojov na rozpoznanie, monitorovanie a riadenie bezpečnostných incidentov, na implementáciu Koncepcie, ktorá je prebratím Európskej stratégie pre kybernetickú bezpečnosť, ako aj na zabezpečenie a prevádzkovanie mimoriadne dôležitých infraštruktúr budú na financovanie vybrané cieľové skupiny **využívať aj finančné prostriedky z Operačného programu Integrovaná infraštruktúra,** špecifický cieľ 7.9., ako ďalší možný zdroj financovania.

Národný bezpečnostný úrad bude zabezpečovať plnenie úloh a koordinovať aktivity vyplývajúce z Akčného plánu, priebežne bude analyzovať, prehodnocovať, diskutovať a hodnotiť plnenie jednotlivých oblastí a úloh a to v spolupráci s ostatnými zainteresovanými subjektmi. Akčný

plán môže byť aktualizovaný a priebežne vyhodnocovaný na základe výsledkov správy o stave kybernetickej bezpečnosti.

Zoznam použitých skratiek

BR SR	Bezpečnostná rada Slovenskej republiky
CCD CoE	NATO Cooperative Cyber Defence Centre of Excellence (Centrum výnimočnosti pre kybernetickú obranu)
CECSP	Central European Cyber Security Platform (Stredoeurópska platforma pre kybernetickú bezpečnosť)
CERT	Computer Emergency Response Team
CSIRT	omputer Security Incident Response Team
DC	Datacentrum
ENISA	European Union Agency for Network and Information Security (Európska agentúra pre bezpečnosť sietí a informácií)
EÚ	Európska únia
MF SR	Ministerstvo financií Slovenskej republiky
MK SR	Ministerstvo kultúry Slovenskej republiky
MO SR	Ministerstvo obrany Slovenskej republiky
MS SR	Ministerstvo spravodlivosti Slovenskej republiky
MŠVVaŠ	Ministerstvo školstva, vedy, výskumu a športu Slovenskej republiky
MV SR	Ministerstvo vnútra Slovenskej republiky
MZVaEZ	Ministerstvo zahraničných vecí a európskych záležitostí Slovenskej republiky
NASES	Národná agentúra pre sieťové a elektronické služby
NATO	Organizácia severoatlantickej zmluvy (North Atlantic Treaty Organisation)
NBAC	Národné bezpečnostné analytické centrum
NBÚ	Národný bezpečnostný úrad
NJRI	Národná jednotka na riešenie incidentov
SR	Slovenská republika
ÚOŠS	ústredné orgány štátnej správy
ÚPVS	Ústredný portál verejnej správy
ÚV SR	Úrad vlády Slovenskej Republiky
VPA	Vecne príslušná autorita pre kybernetickú bezpečnosť