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

Obsah

Úvod

Priorita kybernetickej bezpečnosti je zdôraznená vo viacerých koncepčných a strategických dokumentoch Európskej únie (ďalej len „EÚ“) a Organizácie Severoatlantickej zmluvy (ďalej len „NATO“), ako aj v dokumentoch ďalších významných organizácií po celom svete, kde sa narušenie kybernetického priestoru chápe ako jedna z kľúčových hrozieb súčasnosti. Z tohto dôvodu progresívne vlády štátov pristupujú k zavedeniu účinných opatrení zameraných na budovanie a posilňovanie kybernetických spôsobilostí s cieľom predchádzať, zaznamenávať, brániť sa a zotavovať sa z prípadných kybernetických útokov. EÚ v rámci svojho kybernetického priestoru zadefinovala východiská a ciele kybernetickej bezpečnosti v podobe Stratégie kybernetickej bezpečnosti EÚ, pričom princípy, ciele, priority a postupy budovania kybernetickej bezpečností v Slovenskej republike, okrem tohto významného dokumentu, nadväzujú najmä na strategické a legislatívne dokumenty

- Národná stratégia pre informačnú bezpečnosť v Slovenskej republike, schválená uznesením vlády SR č. 570/2008,
- Koncepcia šifrovej ochrany informácií, schválená uznesením vlády SR č. 771/2008,
- Návrh systému vzdelávania v oblasti informačnej bezpečnosti/kybernetickej bezpečnosti v Slovenskej republike, schválený uznesením vlády SR č. 391/2009,
- Návrh organizačného, personálneho, materiálno-technického a finančného zabezpečenia na vytvorenie špecializovanej jednotky pre riešenie počítačových incidentov v Slovenskej republike – CSIRT.SK, schválený uznesením vlády SR č. 479/2009,
- Návrh Akčného plánu na roky 2009 až 2013 k dokumentu Národná stratégia pre informačnú bezpečnosť v Slovenskej republike, schválený uznesením vlády SR č. 46/2010,
- Legislatívny zámer zákona o informačnej bezpečnosti, schválený uznesením vlády SR č. 136/2010,
- Stratégia Európskej únie pre kybernetickú bezpečnosť: Otvorený, bezpečný a chránený kybernetický priestor, schválená Európskou komisiou 07.02.2013,
- Smernica EP a Rady 2013/40/EÚ o útokoch na informačné systémy, ktorou sa nahrádza rámcové rozhodnutie rady 2005/222/SVV,
- Správy o plnení úloh z Národnej stratégie pre informačnú bezpečnosť v Slovenskej republike a Akčného plánu z rokov 2009 až 2014, predložené na rokovanie vlády SR,
- Návrh smernice Európskeho parlamentu a Rady o opatreniach na zabezpečenie vysokej úrovne bezpečnosti sietí a informácií v Únii (pracovný materiál),
- Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020 (ďalej len „Koncepcia“), schválená uznesením vlády SR č. 328/2015,
- Správa o plnení úloh vyplývajúcich z materiálu Príprava Slovenskej republiky na plnenie úloh v oblasti kybernetickej obrany vyplývajúcich z cieľov spôsobilostí Slovenskej republiky, schválená uznesením vlády SR č. 334/2015.

Vytváranie podmienok pre budovanie národných kybernetických spôsobilostí bolo charakterizované aj ďalšími aktivitami v oblasti prípravy, tvorby a predkladania strategických a koncepčných materiálov pre oblasť kybernetickej bezpečnosti v Slovenskej republike. Preto

úlohou B.3 z uznesenia vlády SR č. 328/2015 zo 17. júna 2015 bolo riaditeľovi Národného bezpečnostného úradu uložené 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 časové etapy v horizonte ich plnenia v roku 2015 a v rokoch 2016-2020. Kľúčové úlohy, a to najmä z hľadiska krátkodobého horizontu ich plnenia, resp. úlohy v prípravnej fáze boli plnené do konca roka 2015.

Sú to predovšetkým

- prijatie 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, ktorým bol Národný bezpečnostný úrad ustanovený ako ústredný orgán štátnej správy pre kybernetickú bezpečnosť;
- zriadenie Komisie pre kybernetickú bezpečnosť, ktorej štatút prerokovala vláda Slovenskej republiky a vzala na vedomie (č. m. UV-33740/2015);
- prijatie 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, ktorým bol zriadený výbor pre kybernetickú bezpečnosť Bezpečnostnej rady Slovenskej republiky.

Plnenie úloh v druhej etape (2016 – 2020) je podrobne rozpracované v Akčnom pláne. Gestorom Akčného plánu je Národný bezpečnostný úrad, pričom úspešné plnenie definovaných úloh si vyžaduje plnú súčinnosť aj ďalších subjektov. Na základe toho sa zodpovednosť za plnenie úloh ukladá aj iným ústredným orgánom štátnej správy, vrátane subjektov v rozsahu nich vecnej pôsobnosti.

Plnenie úloh v Akčnom pláne na roky 2016-2020 je rozdelené do siedmych strategických oblastí, ktorými sú:

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.

V rámci jednotlivých oblastí Akčný plán definuje úlohy, spôsob ich realizácie, určuje zodpovedný subjekt, súčinnostný subjekt, 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 taktiež definuje cieľ, aby sa súkromný sektor, akademická obec, ako aj občianska spoločnosť aktívne zúčastňovali na formovaní a realizácii politiky Slovenskej republiky v oblasti kybernetickej bezpečnosti a aby bola zabezpečená efektívna spolupráca na národnej i 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.

Jednotlivé úlohy Akčného plánu predstavujú dynamické celky, ktoré môžu byť priebežne aktualizované na základe prieskumov a zistení stavu v oblasti kybernetickej bezpečnosti. Rozsah úloh v jednotlivých oblastiach, časový rámec ich plnenia, vrátane zodpovedných subjektov sú rozpracované v nasledujúcej tabuľke úloh.

Tabuľka úloh

1. OBLASŤ: VYTVORENIE INŠTITUCIONÁLNEHO RÁMCA RIADENIA KYBERNETICKEJ BEZPEČNOSTI

Číslo úlohy	Úloha	Spôsob realizácie	Zodpovedný subjekt	Súčinnostný subjekt	Časový rámec realizácie
1.1.	Pripraviť návrh na vytvorenie formálnej platformy pre spoluprácu.	Zabezpečovať podmienky pre činnosť komisie pre kybernetickú bezpečnosť a jej pracovných skupín zriadených na platforme spolupráce verejnej správy, akademickej obce, vedeckých kruhov a súkromnej sféry.	NBÚ	AKOB ZaA	priebežne
		Zriadiť pracovný výbor pre kybernetickú bezpečnosť pri BR SR a zabezpečovať organizačné podmienky pre jeho činnosť.	ÚV SR	NBÚ	2016 a priebežne
1.2.	Vytvoriť podmienky pre výkon kompetencií vecne príslušných autorít pre kybernetickú bezpečnosť vo svojej pôsobnosti.	Vypracovať návrh na personálne a materiálno-technické predpoklady pre výkon kompetencií vecne príslušných autorít pre kybernetickú bezpečnosť.	VPA		04/2016
		Vytvárať podmienky pre materiálno-technické zabezpečenie a konsolidáciu organizačného a personálneho zabezpečenia a plnenia základných úloh vecne príslušných autorít.	VPA		priebežne
		Zabezpečiť spoluprácu vecne príslušných autorít pre kybernetickú bezpečnosť.	ÚOŠS SR		2016-2020
1.3.	Zabezpečiť inštitucionálny rámec riadenia kybernetickej bezpečnosti.	Vytvoriť národné centrum pre kybernetickú bezpečnosť v pôsobnosti úradu.	NBÚ		2017
		Vytvoriť medzirezortnú pracovnú skupinu (zoskupenie) na riešenie rozsiahlych počítačových/kybernetických útokov a tímu rýchleho nasadenia a v prípade potenciálneho ohrozenia kybernetického priestoru SR operatívne zasahovať.	NBÚ	MF SR MV SR MO SR SIS	2016 a priebežne
1.4.	Budovať spôsobilosti kybernetickej bezpečnosti.	Dobudovať spôsobilosti CSIRT.MIL.SK, ako jednotky na riešenie incidentov, pre účely obrany SR, spôsobilosti aktívnej kybernetickej obrany, spôsobilosti v mobilných sieťach OS SR a implementáciu prvkov kybernetickej bezpečnosti do rezortných dátových sietí.	MO SR		2016-2020
		Dobudovať vybrané spôsobilosti CSIRT.SK (vládnej jednotky) v DataCentre v pôsobnosti Ministerstva financií SR.	MF SR	DC/CSIRT.SK	2016-2020

	Navrhnúť organizačné, personálne, materiálno-technické a finančné zabezpečenie jednotky na riešenie incidentov vo svojej pôsobnosti.	ÚV SR	NASES	04/2016
	Zriadiť jednotku vo svojej pôsobnosti a dobudovať jej spôsobilosti.	ÚV SR	NASES	2017
	Zabezpečiť zriadenie a výkon činností útvarov na riešenie incidentov typu CERT/CSIRT alebo zabezpečiť tento výkon činnosti prostredníctvom existujúcich útvarov/jednotiek pôsobiacich v pôsobnosti inej vecne príslušnej autority v súlade s ustanoveniami zákona o kybernetickej bezpečnosti.	VPA		2017-2020
1.5. Vytvoriť rámec riadenia kybernetickej bezpečnosti v čase núdzového stavu, výnimočného stavu, vojnového stavu a vojny.	Navrhnúť inštitucionálne riadenie kybernetickej bezpečnosti v núdzovom stave, výnimočnom stave, vojnovom stave a stave vojny.	NBÚ	MO SR MV SR BR SR	2017/18
	Navrhnúť kontingenčný plán prechodu zodpovednosti za riadenie kybernetickej bezpečnosti v čase mieru, núdzového a výnimočného stavu do vojnového stavu a stavu vojny podľa ústavného zákona č. 227/2002 Z. z.	NBÚ	MO SR MV SR BR SR	2017/18
1.6. Vytvoriť medzirezortný/nadrezortný rozpočtový program „Ochrana kybernetického priestoru Slovenskej republiky“.	Predložiť na schválenie vláde SR nadrezortný rozpočtový program „Ochrana kybernetického priestoru Slovenskej republiky.“	NBÚ	MF SR MV SR MDVaRR SR MŠVVaŠ SR MO SR ÚV SR SIS	06/2016
	Predložiť na rokovanie vlády SR implementačný 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 nadrezortného rozpočtového programu.	NBÚ	MF SR MV SR MDVaRR SR MO SR ÚV SR NASES	12/2016

2. OBLASŤ: VYTVORENIE A PRIJATIE LEGISLATÍVNEHO RÁMCA KYBERNETICKEJ BEZPEČNOSTI

Číslo úlohy	Úloha	Spôsob realizácie	Zodpovedný subjekt	Súčinnostný subjekt	Časový rámec realizácie
2.1.	Vytvoriť legislatívne podmienky pre oblasť kybernetickej bezpečnosti.	Pripraviť návrh zákona o kybernetickej bezpečnosti a predložiť ho do formálneho legislatívneho procesu.	NBÚ	MF SR VPA NASES CSIRT.SK	06/2016
		Predložiť návrh zákona o kybernetickej bezpečnosti na rokovanie vlády SR.	NBÚ	MF SR	09/2016
		Vytvárať podmienky pre implementáciu príslušných ustanovení zákona o kybernetickej bezpečnosti vo svojej pôsobnosti.	Povinné osoby		od 2017
2.2.	Zosúladiť súvisiace právne prepisy so zákonom o kybernetickej bezpečnosti.	Vykonať analýzu prostredia a pripraviť zoznam právnych predpisov s návrhom ich novelizácie a časovým harmonogramom.	NBÚ	ÚOŠS SR	06/2017
2.3.	Pripraviť, vykonávacie predpisy k zákonu o kybernetickej bezpečnosti a zabezpečiť ich legislatívny proces (schválenie).	Pripraviť vykonávacie predpisy upravujúce podrobnosti k oblastiam na základe blanketnej normy v zákone o kybernetickej bezpečnosti.	NBÚ	ÚOŠS SR	06/2017
2.4.	Vydávať štandardy, metodiky a metodické usmernenia v oblasti kybernetickej bezpečnosti.	V pôsobnosti Komisie pre kybernetickú bezpečnosť NBÚ zriadiť pracovné skupiny pre: - kybernetický zločin a počítačovú kriminalitu - metodiku a štandardy - terminológiu v oblasti KB.	NBÚ		04/2016
		Vydávať štandardy, metodiky a metodické usmernenia.	NBÚ	ÚNMS SR VPA SIS	priebežne
		Zriadiť centrálny prístupový bod k normám a štandardom pre ochranu prvkov kritickej infraštruktúry a zabezpečovať pravidelnú aktualizáciu jeho obsahu.	NBÚ	ÚNMS DC SNAS NASES	06/2017
2.5.	Terminológia v oblasti kybernetickej bezpečnosti.	Aktualizovať slovník krízového riadenia v súlade s výstupmi Komisie pre kybernetickú bezpečnosť pri NBÚ v oblasti terminológie a doplniť ho o nové pojmy.	ÚV SR	VPA NBÚ BR SR	06/2016
		Vytvoriť terminologický výkladový slovník za účelom zjednotenia pojmov pre účely tvorby koncepčných, strategických a legislatívnych materiálov v oblasti kybernetickej bezpečnosti a zabezpečovať jeho aktualizáciu.	NBÚ	AKOB	06/2017 a potom priebežne

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

Číslo úlohy	Úloha	Spôsob realizácie	Zodpovedný subjekt	Súčinnostný subjekt	Časový rámec realizácie
3.1.	Vytvoriť metodiku hodnotenia rizík v kybernetickom priestore.	Vypracovať metodiku hodnotenia rizík pre oblasť kybernetickej bezpečnosti na národnej úrovni.	NBÚ	AKOB ZaA	12/2016
		Vytvoriť postupy pre analýzu stavu, vyhodnocovať ho a navrhovať bezpečnostné opatrenia na odstránenie/minimalizáciu rizík a možných krízových stavov v priestore štátu.	NBÚ		2016 (každoročne)
3.2.	V rámci mechanizmu prevencie zaviesť jednotné opatrenia z úrovne vecne príslušných autorít.	Zaviesť opatrenia na minimalizáciu potenciálnych rizík a krízových stavov vo svojej pôsobnosti.	VPA		2018
3.3.	Vytvoriť procesy a mechanizmy pri koordinácii zabezpečovania ochrany významných informačných aktív štátu na národnej úrovni.	Vytvoriť metodiku pre spoločné postupy a podporu (hotline) za účelom zabezpečenia prevencie a pripravenosti proti narušeniu informačných aktív kritickej infraštruktúry.	MF SR	NBÚ MV SR DC/CSIRT.SK	2016
3.4.	Vytvoriť a implementovať systém včasného varovania a reakcie na incidenty.	Implementovať jednotný systém včasného varovania, reakcie na incidenty a výmeny informácií podľa časového harmonogramu za účelom zníženia rizík vyplývajúcich z hrozieb informačných a komunikačných systémov a zabezpečovať jeho nepretržitú prevádzku v súlade s plnením úlohy „OAS02 Medzirezortného programu na ochranu kritickej infraštruktúry v SR.“	NBÚ	DC/CSIRT.SK VPA/JRI	2016-2020
		Zriadiť Národný portál pre kybernetickú bezpečnosť ako súčasť ÚPVS.	ÚV SR	NASES	2017
3.5.	V rámci mechanizmu reakcie na bezpečnostné incidenty navrhnúť minimálne bezpečnostné opatrenia pre jednotlivé kategórie informačných aktív a zabezpečiť ich implementáciu.	Zaviesť jednotné opatrenia na národnej úrovni, ktorých cieľom bude kvalifikovane a efektívne reagovať na bezpečnostné incidenty.	NBÚ	VPA	2018
		Navrhnúť a zaviesť pravidlá pre blokovanie útokov za účelom zvýšenia obranyschopnosti SR voči kybernetickým útokom na významné informačné systémy z externého prostredia/internetu, najmä voči šíreniu škodlivého kódu zo sietí infikovaných počítačov a šíreniu škodlivej aktivity z IP adresného rozsahu SR.	NBÚ	DC/CSIRT.SK NASES SIS	2016

		Vytvoriť mechanizmus na eskaláciu na zodpovedajúce útvary krízového riadenia a na vládu SR, kompatibilné s mechanizmami európskej úrovne a NATO a koordináciu riešenia rozsiahlych bezpečnostných incidentov/útokov, krízových stavov na úrovni štátu podľa štandardných operačných procedúr za účelom zefektívnenia koordinácie postupov riešenia rozsiahlych bezpečnostných incidentov.	NBÚ	MV SR MO SR MDVaRR SR MZVaEZ SR SIS DC/CSIRT.SK NASES	2017
3.6.	Aktualizovať plány riešenia krízových situácií pre oblasť kybernetickej bezpečnosti.	Aktualizovať katalógové listy a doplniť ich tak, aby reflektovali na bezpečnostné incidenty v rámci kybernetického priestoru.	NBÚ		2017
3.7.	Pravidelne vykonávať ohodnotenie úrovne bezpečnosti vo vládnych sieťach a kritických infraštruktúrach.	Vykonávať interné a externé penetračné testy informačných systémov vybraných organizácií verejnej správy, vrátane prvkov kritickej informačnej infraštruktúry a ďalších významných informačných systémov.	MF SR	ÚOŠS DC/CSIRT.SK Prevádzko-vatelia prvkov KII SIS	priebežne

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

Číslo úlohy	Úloha	Spôsob realizácie	Zodpovedný subjekt	Súčinnostný 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).	MŠVVaŠ SR	NBÚ MO SR SIS MV SR 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	MO SR SIS MV SR NASES	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 jednotlivých stupňov škôl.	MŠVVaŠ SR	MPSVaR SR	06/2017
4.5.	Systematicky zvyšovať povedomie o aspektoch kybernetickej bezpečnosti.	Zabezpečiť šírenie osvety o bezpečnostných hrozbách, bezpečnostných rizikách a pravidlách správania sa v informačných systémoch verejnej správy	NBÚ	MF SR MK SR MPSVaR SR NASES	priebežne
4.6.	Zabezpečiť školenie o kybernetickej bezpečnosti.	V rámci rozvoja siete Govnet a služieb ÚPVS rozšíriť obsah existujúcich školení aj o oblasť kybernetickej bezpečnosti.	ÚV SR	NASES	2016-2020
		Rozšíriť existujúci projekt vzdelávania zamestnancov verejnej správy o ďalšie špecifické oblasti a zabezpečiť pokračovanie vzdelávania.	NBÚ	AKOB	2017
		Realizovať školenia pracovníkov verejnej správy v oblasti ochrany informačných aktív voči kybernetickým útokom z externého prostredia.	MF SR	DC/CSIRT.SK	
4.7.	Vytvoriť študijné programy v rámci celoživotného vzdelávania profesionálnych vojakov.	V rámci Centra vzdelávania Akadémie ozbrojených síl vytvoriť programy pre všetkých profesionálnych vojakov – špecialistov IKT so zameraním na kybernetickú bezpečnosť.	MO SR		2016-2017
		V rámci Centra vzdelávania Akadémie ozbrojených síl vytvoriť programy pre všetkých profesionálnych vojakov so zameraním na kybernetickú bezpečnosť.	MO SR		2017-2019
4.8.	Zabezpečiť vzdelávanie v oblasti informačnej a kybernetickej bezpečnosti v rámci justičných orgánov.	Zaviesť minimálnu úroveň systematického vzdelávania pre všetkých sudcov, prokurátorov na všetkých úrovniach.	MS SR	GP SR JA SR Súdna rada	2016-2020
		Zaviesť rozšírené vzdelávanie pre vybraných sudcov, prokurátorov na všetkých úrovniach.	MS SR	GP SR JA SR Súdna rada	2016-2020

4.9.	Zabezpečiť vzdelávanie v oblasti kybernetickej bezpečnosti v rámci vyšetrovacích orgánov.	Zaviesť minimálnu úroveň systematického vzdelávania v oblasti kybernetickej bezpečnosti pre vyšetrovateľov na všetkých úrovniach.	MV SR	APZ	2016-2020
		Zaviesť rozšírené vzdelávanie v oblasti kybernetickej bezpečnosti pre vybraných vyšetrovateľov na všetkých úrovniach.	MV SR	APZ	2016-2020
4.10.	Zabezpečiť vytvorenie popisu kvalifikácie pre oblasť informačnej a kybernetickej bezpečnosti v rámci národnej sústavy kvalifikácií v SR.	Vykonať analýzu existujúceho stavu pre oblasť bezpečnosti IKT a v spolupráci s relevantnými ústrednými orgánmi štátnej správy pripraviť návrh doplnenia zoznamu kvalifikácií a predložiť materiál na rokovanie vlády SR.	NBÚ	MPSVaR SR	2017

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

Číslo úlohy	Úloha	Spôsob realizácie	Zodpovedný subjekt	Súčinnostný subjekt	Časový rámec realizácie
5.1.	Vytvoriť efektívny model spolupráce na národnej úrovni medzi jednotlivými subjektmi kybernetickej bezpečnosti.	Vypracovať návrh spolupráce na národnej úrovni medzi pracoviskami na riešenie incidentov (CERT/CSIRT a pod.) za účelom výmeny a zdieľania informácií najmä o bezpečnostných incidentoch.	NBÚ	VPA	2016
		Vytvoriť bezpečný komunikačný kanál prostredníctvom ktorého budú jednotky pre riešenie incidentov automatizovane prijímať a spracovávať hlásenia o závažných kybernetických bezpečnostných incidentoch.	NBÚ	DC NASES	2017
5.2.	Implementovať systém nahlasovania a riešenia bezpečnostných incidentov.	Implementovať on-line systém nahlasovania a riešenia bezpečnostných incidentov.	NBÚ	DC/CSIRT.SK NASES	2017

6. OBLASŤ: AKTÍVNA MEDZINÁRODNÁ SPOLUPRÁCA

Číslo úlohy	Úloha	Spôsob realizácie	Zodpovedný subjekt	Súčinnostný subjekt	Časový rámec realizácie
6.1.	V rámci členstva v EÚ sa aktívne zúčastňovať na príprave a realizácii legislatívnych a nelegislatívnych iniciatív týkajúcich sa kybernetickej bezpečnosti.	Zabezpečiť aktívnu účasť expertov v dotknutých pracovných skupinách a výboroch inštitúcií EÚ predovšetkým ku negociácii a implementácii smernice o sieťovej a informačnej bezpečnosti.	NBÚ	MZVaEZ SR MF SR	priebežne
		Zabezpečovať aktívnu účasť expertov na programoch, projektoch a ďalších iniciatívach týkajúcich sa informačnej/kybernetickej bezpečnosti v kontexte viacročného finančného rámca EÚ 2014-2020 a v kontexte implementácie Stratégie kybernetickej bezpečnosti EÚ a jednotného digitálneho trhu.	NBÚ	MZVaEZ SR MF SR	priebežne
		Spolupracovať a aktívne sa podieľať na činnostiach a aktivitách medzinárodných platforiem v rámci medzinárodných organizácií.	MZVaEZ SR	NBÚ MF SR	2016-2020
6.2.	V rámci členstva v NATO podporovať spoluprácu s NATO v oblasti kybernetickej obrany.	Podpísať Memorandum o spolupráci v oblasti kybernetickej obrany.	NBÚ	MO SR	02/2016
		Podporovať spoluprácu s NATO v oblasti kybernetickej obrany, najmä s ohľadom na reakcie na počítačové bezpečnostné incidenty a výmenu technických informácií o hrozbách a zraniteľnostiach.	NBÚ	MO SR MZVaEZ SR	2016-2020
		Podpísať „Statement of Interest“ o pristúpení SR k NATO projektu MISP (Malware Information Sharing Platform).	NBÚ	MO SR MZVaEZ SR	06/2016
6.3.	V rámci stredoeurópskeho priestoru rozvíjať vzťahy a nadväzovať bilaterálne spoluprácu s vybranými krajinami v oblasti kybernetickej bezpečnosti.	Aktívne sa podieľať, rozvíjať a podporovať spoluprácu v rámci krajín V4, predovšetkým prostredníctvom Stredoeurópskej platformy kybernetickej bezpečnosti (Central European Cyber Security Platform, CECSP).	NBÚ	DC MO SR	priebežne
		Nadväzovať a prehlbovať bilaterálne spolupráce s krajinami, ktoré vykonávajú podobné aktivity ako SR.	NBÚ	MZVaEZ SR	priebežne
6.4.	Zapájať sa a zúčastňovať sa na medzinárodných kybernetických cvičeniach.	Zabezpečiť pravidelnú aktívnu účasť na medzinárodných kybernetických cvičeniach (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 Centre of Excellence – CCD CoE).	Navýšiť personálne kapacity zástupcov SR vyslaných na plnenie služobných povinností do CCD CoE.	MO SR		2018
		Na základe ponuky školení a vzdelávacích aktivít CCD CoE pravidelne informovať subjekty a umožniť účasť na predmetných aktivitách.	MO SR		priebežne

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

Číslo úlohy	Úloha	Spôsob realizácie	Zodpovedný subjekt	Súčinnostný 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	AKOB MF SR NASES	2016-2020
		Podporovať výskumnú činnosť v oblasti kybernetickej bezpečnosti prostredníctvom prostriedkov vyčlenených pre Európsky výskumný priestor.	MŠVVaŠ SR	AKOB MF SR NASES	2016-2020
7.2.	Podporovať budovanie forenzných pracovísk.	Podporovať budovanie nových špecializovaných pracovísk za účelom posilnenia ochrany významných informačných aktív štátu, s následným využitím ich poznatkov pre podporu rozvoja vedy a výskumu v oblasti kybernetickej bezpečnosti.	NBÚ		2016-2020
		Vytvárať forenzné pracoviská vo svojej pôsobnosti zamerané na vykonávanie analytických činností pri riešení bezpečnostných incidentov/útokov a vykonávaním úkonov súvisiacich so zberom a vyhodnocovaním digitálnych stôp v organizácii pre poskytovanie služieb organizáciám štátnej správy a zabezpečovať ich prevádzku.	ÚOŠS		2016-2020

Záver

Akčný plán obsahuje návrh úloh, ktorých cieľom je zabezpečiť primeranú ochranu kybernetického priestoru štátu pred potenciálnymi hrozbami, ktorých uplatnením by mohli vzniknúť Slovenskej republike významné alebo nenahraditeľné škody, a tak by mohla byť narušená dôveryhodnosť štátu či organizácie. Akčný plán je jeden zo základných dokumentov definujúcich zoznam úloh na obdobie rokov 2016 až 2020 zameraných na tvorbu právnych predpisov, štandardov, metodických pokynov, pravidiel, bezpečnostných politík, ako aj iných aktivít potrebných k zaisteniu ochrany a obrany národného kybernetického priestoru. Plnením úloh, ktoré môžu byť v dôsledku dynamicky sa vyvíjajúceho prostredia priebežne dopĺňané, budú vytvorené predpoklady pre ucelený, koordinovaný a efektívny systém ochrany kybernetického priestoru Slovenskej republiky.

Návrh úloh vychádza z reálneho prostredia v SR, ktorý bol sformulovaný do strategických cieľov Koncepcie. Plnenie úloh obsiahnutých v Akčnom pláne je uvažované v rozsahu rokov 2016-2020. Realizácia úloh Akčného plánu predpokladá krytie finančnými prostriedkami z viacerých zdrojov operačných programov, ktorých rámec financovania vychádza zo Stratégie informačnej bezpečnosti v SR, vrátane čiastkového financovania v rámci schválených limitov rozpočtových kapitol ÚOŠS SR. Aktivity zamerané na vytváranie nástrojov na rozpoznanie, monitorovanie a riadenie bezpečnostných incidentov, zabezpečenie kritickej infraštruktúry a implementáciou opatrení európskej stratégie pre kybernetickú bezpečnosť, si však vyžadujú úpravu legislatívy a jej zosúladenie, čo návrh úloh primerane zohľadňuje.

Predpokladanými zdrojmi financovania aktivít sú predovšetkým:

- Operačný program pre Integrovanú infraštruktúru - OPII v gescii MDVaRR SR,
- Operačný program Výskum a inovácie v gescii MŠVVaŠ SR,
- Operačný program Ľudské zdroje, prioritná os 1: vzdelávanie, v gescii MŠVVaŠ SR / MPSVaR SR,
- Medzirezortný program pre ochranu kritickej infraštruktúry v gescii MV SR,
- Rozpočtová kapitola NBÚ a rozpočtové kapitoly dotknutých subjektov.

Ďalším uvažovaným zdrojom financovania je nadrezortný/medzirezortný program pre Ochranu kybernetického priestoru Slovenskej republiky pod gesciou Národného bezpečnostného úradu. Vypracovanie návrhu programu je zahrnuté do tohto materiálu v úlohe 1.6. Časový rámec čerpania z programu sa predpokladá až v rokoch 2017-2020.

Akčný plán môže byť aktualizovaný a rozšírený o ďalšie relevantné úlohy reflektujúce aktuálny stav prostredia, ktoré podlieha neustálym dynamickým zmenám. Plnenie jednotlivých úloh a ich stav budú priebežne monitorované a vyhodnocované, spravidla na základe ročných vyhodnotení. Súhrnná správa o stave ich plnenia bude predkladaná vláde na vedomie každoročne.

Zoznam použitých skratiek

APZ	Akadémia Policajného zboru v Bratislave
AKOB	Akademická obec
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 (Jednotka pre riešenie počítačových bezpečnostných incidentov)
CSIRT	Computer Security Incident Response Team (Jednotka pre riešenie počítačových bezpečnostných incidentov)
CSIRT.SK	Jednotka pre riešenie počítačových incidentov zriadená MF SR
DC	DataCentrum
EÚ	Európska únia
GP SR	Generálna prokuratúra Slovenskej republiky
IKT	Informačné a komunikačné technológie
JA SR	Justičná akadémia Slovenskej republiky
JRI	Jednotka na riešenie incidentov
KI	Kritická infraštruktúra
KII	Kritická informačná infraštruktúra
MDVaRR SR	Ministerstvo dopravy, výstavby a regionálneho rozvoja Slovenskej republiky
MF SR	Ministerstvo financií Slovenskej republiky
MK SR	Ministerstvo kultúry Slovenskej republiky
MO SR	Ministerstvo obrany Slovenskej republiky
MPSVaR SR	Ministerstvo práce sociálnych vecí a rodiny Slovenskej republiky
MS SR	Ministerstvo spravodlivosti Slovenskej republiky
MŠVVaŠ SR	Ministerstvo školstva, vedy, výskumu a športu Slovenskej republiky
MV SR	Ministerstvo vnútra Slovenskej republiky
MZVaEZ SR	Ministerstvo zahraničných vecí a európskych záležitostí Slovenskej republiky
NASES	Národná agentúra pre sieťové a elektronické služby
NATO	North Atlantic Treaty Organisation (Organizácia Severoatlantickej zmluvy)
NBAC	Národné bezpečnostné analytické centrum
NBÚ	Národný bezpečnostný úrad
SIS	Slovenská informačná služba
SNAS	Slovenská národná akreditačná spoločnosť
SR	Slovenská republika
ÚNMS SR	Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky
ÚOŠS	Ústredné orgány štátnej správy
ÚPVS	Ústredný portál verejnej správy
ÚV SR	Úrad vlády Slovenskej Republiky
VPA	Vecne príslušná autorita pre kybernetickú bezpečnosť (vecne príslušné autority definované v Akčnom pláne sú ÚOŠS SR v zmysle zákona č. 45/2011 Z. z. o kritickej infraštruktúre, resp. aj ďalšie subjekty podľa iných osobitných predpisov
ZaA	Združenia a asociácie