Porovnanie úloh ktoré NBÚ vyplývajú z Akčného plánu a zo Zákona o kybernetickej bezpečnosti

Úlohy a kompetencie NBÚ Úrad v oblasti kybernetickej bezpečnosti	Úlohy NBÚ z Akčného plánu	Realizácia
a) riadi a koordinuje výkon štátnej správy,	1.1.Zabezpečiť inštitucionálny rámec riadenia kybernetickej bezpečnosti. • Vytvoriť národné centrum pre kybernetickú bezpečnosť v pôsobnosti úradu. • 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. 1.5 Vytvoriť rámec riadenia kybernetickej bezpečnosti v čase núdzového stavu, výnimočného stavu, vojnového stavu a vojny. 1.6. Vytvoriť medzirezortný/nadrezortný rozpočtový program „Ochrana kybernetického priestoru Slovenskej republiky“. 2.1. Vytvoriť legislatívne podmienky pre oblasť kybernetickej bezpečnosti. 2.2. Zosúladiť súvisiace právne prepisy so zákonom o kybernetickej bezpečnosti. 2.3. Pripraviť, vykonávacie predpisy k zákonu o kybernetickej bezpečnosti a zabezpečiť ich legislatívny proces (schválenie).	nie nie nie nie zákon nie nie

	4.10. Zabezpečiť vytvorenie popisu kvalifikácie pre oblasť informačnej a kybernetickej bezpečnosti v rámci národnej sústavy kvalifikácií v SR.	nie
b) určuje štandardy, operačné postupy, vydáva metodiku a politiku správania sa v kybernetickom priestore,	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. • Vydávať štandardy, metodiky a metodické usmernenia. 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. • Vytvoriť terminologický výkladový slovník za účelom zjednotenia pojmov pre účely tvorby koncepčných, strategických a legislatívnych materiálov v oblasti kybernetickej bezpečnosti a zabezpečovať jeho aktualizáciu.	nie neboli zriadené nie 20 pojmov slovník vznikol bez pričinenia NBÚ
c) určuje zásady predchádzania kybernetickým bezpečnostným incidentom a zásady ich riešenia,	3.1. Vytvoriť metodiku hodnotenia rizík v kybernetickom priestore. • Vypracovať metodiku hodnotenia rizík pre oblasť kybernetickej bezpečnosti na národnej úrovni. • Vytvoriť postupy pre analýzu stavu, vyhodnocovať ho a navrhovať bezpečnostné opatrenia na odstránenie/minimalizáciu rizík a možných krízových stavov v priestore štátu.	nie nie
d) vypracúva národnú stratégiu kybernetickej		

	bezpečnosti a ročnú správu o stave kybernetickej bezpečnosti v Slovenskej republike v spolupráci s príslušnými štátnymi orgánmi,		
e)	je národným kontaktným miestom pre kybernetickú bezpečnosť pre zahraničie a zabezpečuje spoluprácu s jednotnými kontaktnými miestami iných členských štátov Európskej únie a Organizácie severoatlantickej zmluvy,		
f)	plní notifikačné a nahlasovacie povinnosti voči príslušným orgánom Európskej únie a Organizácie severoatlantickej zmluvy a podieľa sa a podporuje vytváranie partnerstiev na národnej a medzinárodnej úrovni v oblasti kybernetickej bezpečnosti,		
g)	zabezpečuje členstvo Slovenskej republiky v skupine pre spoluprácu a v sieti jednotiek CSIRT,		
h)	v spolupráci s Ministerstvom zahraničných vecí a európskych záležitostí Slovenskej republiky rozvíja medzinárodnú spoluprácu a sleduje vplyvy aktivít v oblasti kybernetickej bezpečnosti na zahraničnopolitické záujmy Slovenskej republiky a partnerov v rámci Európskej únie a Organizácie severoatlantickej zmluvy,	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. • 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. 6.2. V rámci členstva v NATO podporovať spoluprácu s NATO v oblasti kybernetickej obrany. 6.3. V rámci stredoeurópskeho priestoru rozvíjať vzťahy a nadväzovať bilaterálne spoluprácu	rokovaní sa zúčastňovali (ak vôbec) zástupcovia/zástupca NBÚ informácie nie sú dostupné

	s vybranými krajinami v oblasti kybernetickej bezpečnosti. 6.4. Zapájať sa a zúčastňovať sa na medzinárodných kybernetických cvičeniach.	
i) spolupracuje s ústrednými orgánmi a jednotkami CSIRT, prevádzkovateľmi základných služieb a poskytovateľmi digitálnych služieb pri plnení úloh podľa tohto zákona,		
j) spravuje a prevádzkuje jednotný informačný systém kybernetickej bezpečnosti,	3.4. Vytvoriť a implementovať systém včasného varovania a reakcie na incidenty. 5.2. Implementovať systém nahlasovania a riešenia bezpečnostných incidentov.	nie
k) na základe oznámenia ústredného orgánu, prevádzkovateľa základnej služby, poskytovateľa digitálnej služby, alebo z vlastnej iniciatívy určuje 1. základnú službu a zaraďuje ju do zoznamu 2. digitálnu službu a zaraďuje ju do zoznamu digitálnych služieb, 3. poskytovateľa digitálnej služby a zaraďuje ho do registra poskytovateľov digitálnych služieb, 4. prevádzkovateľa základnej služby a zaraďuje ho do registra prevádzkovateľov základných služieb,		
l) vedie a spravuje 1. zoznam základných služieb, 2. register prevádzkovateľov základných služieb, 3. zoznam digitálnych služieb, 4. register poskytovateľov digitálnych služieb, 5. zoznam akreditovaných jednotiek		

CSIRT,		
m) systematicky získava, sústreďuje, analyzuje a vyhodnocuje informácie o stave kybernetickej bezpečnosti v Slovenskej republike,		
n) akredituje jednotky CSIRT, okrem Národnej jednotky CSIRT a vládnej jednotky CSIRT a zaraďuje ich do zoznamu akreditovaných jednotiek CSIRT,		
o) plní úlohy príslušného orgánu pre digitálne služby,		
p) zabezpečuje a zodpovedá za koordinované riešenie kybernetických bezpečnostných incidentov na národnej úrovni,	• Vytvoriť národné centrum pre kybernetickú bezpečnosť v pôsobnosti úradu. • 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. • 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.“ 3.6. Aktualizovať plány riešenia krízových situácií pre oblasť kybernetickej bezpečnosti. 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	nie nie nie nie nie

	výmeny a zdieľania informácií najmä o bezpečnostných incidentoch. • Vytvoriť bezpečný komunikačný kanál prostredníctvom ktorého budú jednotky pre riešenie incidentov automatizovane prijímať a spracovávať hlásenia o závažných kybernetických bezpečnostných incidentoch.	nie
q) rieši kybernetické bezpečnostné incidenty, vyhlasuje výstrahu a varovania pred závažným kybernetickým bezpečnostným incidentom, ukladá povinnosť vykonať reaktívne opatrenie a schvaľuje ochranné opatrenie,	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. • 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. • 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	nie nie nie nie
r) zasiela včasné varovania,		
s) prijíma vnútroštátne hlásenia o kybernetických	5.2. Implementovať systém nahlasovania a riešenia	nie

bezpečnostných incidentoch,	bezpečnostných incidentov.	
t) prijíma hlásenia o kybernetických bezpečnostných incidentoch zo zahraničia a zabezpečuje spoluprácu s medzinárodnými organizáciami a orgánmi iných štátov pri riešení kybernetických bezpečnostných incidentov s cezhraničným charakterom,		
u) vykonáva kontrolu, vydáva rozhodnutia o uložení opatrení na nápravu a ukladá pokutu za priestupok alebo iný správny delikt,		
v) vykonáva audit alebo požiada orgán posudzovania zhody o vykonanie auditu u prevádzkovateľa základnej služby,		
w) vydáva znalostné štandardy a v spolupráci s Ministerstvom školstva, vedy, výskumu a športu Slovenskej republiky vykonáva a zabezpečuje budovanie bezpečnostného povedomia,	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). 4.5. Systematicky zvyšovať povedomie o aspektoch kybernetickej bezpečnosti. 4.6 Zabezpečiť školenie o kybernetickej bezpečnosti. • Rozšíriť existujúci projekt vzdelávania zamestnancov verejnej správy o ďalšie špecifické oblasti a zabezpečiť pokračovanie vzdelávania. 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	nie nie nie nie

	kvalifikácií a predložiť materiál na rokovanie vlády SR.	
x) koordinuje výskum a vývoj.	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.	nie