**Stanovisko Rady pro výzkum, vývoj a inovace k návrhu materiálu „Národní plán výzkumu a vývoje v kybernetické a informační bezpečnosti do roku 2025“**

1. **Způsob předložení návrhu**

Ředitel Národního úřadu pro kybernetickou bezpečnost zaslal dopisem ze dne 7. ledna 2022 č. j. 9082/2021-NÚKIB-E/110 Radě pro výzkum, vývoj a inovace k připomínkám materiál s názvem „Národní plán výzkumu a vývoje v kybernetické a informační bezpečnosti do roku 2025“.

Návrh byl Radě zaslán ke stanovisku podle § 35 odst. 2 písm. i) zákona č. 130/2002 Sb., o podpoře výzkumu, experimentálního vývoje a inovací z veřejných prostředků a o změně některých souvisejících zákonů (zákon o podpoře výzkumu, experimentálního vývoje a inovací), ve znění pozdějších předpisů.

1. **Charakteristika návrhu**

„Národní plán výzkumu a vývoje v kybernetické a informační bezpečnosti do roku 2025“ předložený Národním úřadem pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) je navázán na Národní strategii kybernetické bezpečnosti České republiky a reaguje na potřebu strategické koordinace výzkumných a vývojových aktivit na poli kybernetické a informační bezpečnosti. Národní plán stanovuje rozvojové cíle, prioritní výzkumné oblasti a konkrétní opatření, které mají za cíl stimulovat výzkumné prostředí v České republice, prohlubovat a posilovat spolupráci mezi akademickou, soukromou a veřejnou sférou ve výzkumu, vývoji a implementaci technologií v praxi a rozvíjet zahraniční spolupráci.

Základní strategický rámec zajišťování kybernetické bezpečnosti v ČR je definován v Národní strategii a jejím Akčním plánu. Tvorba a aktualizace Národního plánu je na základě Akčního plánu v gesci NÚKIB. Národní plán výzkumu a vývoje v kybernetické a informační bezpečnosti do roku 2025 (dále jen “Národní plán”) je úzce navázán na Národní strategii a reaguje na potřebu strategické koordinace výzkumných a vývojových aktivit na poli kybernetické a informační bezpečnosti.

Platnost Národního plánu je stanovena do roku 2025, stejně jako u Strategie a jejího Akčního plánu na období let 2021 až 2025.

Materiál stanovuje následující strategické cíle s ambicí posílit kybernetickou a informační bezpečnost státu prostřednictvím výzkumných a vývojových aktivit:

1. Identifikovat prioritní výzkumné oblasti v kybernetické a informační bezpečnosti a zajistit jejich stabilní podporu prostřednictvím národních a mezinárodních programů VaVaI.
2. Rozvinout podpůrné, analytické a informační zázemí v oblasti VaVaI v kybernetické a informační bezpečnosti a vytvořit efektivní nástroje koordinace této oblasti.
3. Nastavit efektivní zahraniční spolupráci a posílit roli ČR v evropském systému podpory VaVaI.

Cíle jsou rozpracovány do opatření, u těchto opatření jsou uvedeny zodpovědnosti za jejich naplňování (gestor / gestoři), nástroje a indikátory plnění.

Pro dosažení výše uvedených cílů se předpokládá:

* vznik Národního koordinačního centra výzkumu a vývoje v oblasti kybernetické bezpečnosti (plnění úkolů plynoucích z Nařízení Evropského parlamentu a Rady EU č. 2021/887, kterým je zřízené Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center),
  + podpora a šíření výsledků činnosti centra na vnitrostátní, regionální nebo místní úrovni,
  + šíření vzdělávacích programů v oblasti kybernetické bezpečnosti,
  + poskytování finanční podpory třetím stranám, kterým centrum udělilo granty,
* vznik výzkumného programu výlučně pro oblast kybernetické a informační bezpečnosti,
  + ze strany NÚKIB budou učiněny kroky směřující ke vzniku programu VaVaI pro tuto oblast,
* rozvoj platformy pro výzkum a vývoj v kybernetické a informační bezpečnosti,
  + od roku 2021 existující platforma umožňující vzájemné sdílení zkušeností, potřeb a know-how v oblasti VaVaI mezi subjekty působící v kybernetické a informační bezpečnosti.

1. **Výdaje**

Finanční dopady nejsou uvedeny, a to ani v případě uvažovaného programu výzkumu, vývoje a inovací, ani v případě zřízení Národního koordinačního centra výzkumu a vývoje v oblasti kybernetické bezpečnosti.

Rada proto upozorňuje, že finanční dopady je zapotřebí co nejdříve vyjasnit.

1. **Připomínky**
2. **Doporučující připomínka**

K článku 3.2.3 materiálu

Materiál nereflektuje jiné než kryptografické souvislosti vývoje a nasazení kvantových technologií. Z hlediska strategických výzkumných priorit je třeba řešit rovněž ostatní bezpečnostní souvislosti vývoje kvantových počítačů, kvantových sítí a kvantových senzorů.

1. **Doporučující připomínka**

K článku 3.5 materiálu

Mezi výzkumnými potřebami by měl být rovněž výzkum struktury prvků kritické infrastruktury státu (adekvátní politika a postupy krizového řízení mohou být úspěšné pouze, pokud se aplikují v adekvátním rozsahu objektů a institucí).

1. **Doporučující připomínka**

K článku 3.6 materiálu

Téma je popsáno velmi obecně a popis nereflektuje aktuální vývoj české a evropské právní úpravy a praxe ochrany osobních údajů ani nereaguje na změny, které v době realizace strategie přinese jednotná úprava přeshraničního zajišťování elektronických důkazů na základě nařízení o evropských předávacích a uchovávacích příkazech pro elektronické důkazy v trestních věcech.

1. **Závěr**

Rada

* doporučuje Národnímu úřadu pro kybernetickou bezpečnost po zapracování připomínek předložit materiál vládě,
* doporučuje vládě materiál po zapracování připomínek vzešlých z meziresortního připomínkového řízení schválit.

Praha 28. ledna 2022