DIGITÁLNÍ EKONOMIKA A SPOLEČNOST

Implementační plán hlavního cíle č. 5 - DES

IP Zajištění bezpečnosti a důvěry v prostředí digitální ekonomiky a společnosti

[Datum]

Úřad vlády ČR

[Adresa společnosti]

Datum poslední změny dokumentu: **25. 1. 2019**

Verze dokumentu: 1**.1**

Poznámka k verzi:

připomínky NÚKIB zapracovány 25. 1. 2019

# Obsah

[Obsah 1](#_Toc536695782)

[1 Základní informace o implementačním plánu 2](#_Toc536695783)

[1.1 Rekapitulace dílčích cílů implementačního plánu 2](#_Toc536695784)

[1.2 Klasifikace záměrů A, B a C 4](#_Toc536695785)

[1.3 Shrnutí problematiky, celkové přínosy 4](#_Toc536695786)

[1.4 Souhrnné údaje 4](#_Toc536695787)

[1.4.1 Počty záměrů a odhad finanční alokace v rezortech a úřadech (klasifikace A, B, C) 5](#_Toc536695788)

[1.4.2 Počty záměrů a odhad finanční alokace v dílčích cílech (klasifikace A, B, C) 5](#_Toc536695789)

[2 Sestava záměrů dle data ukončení realizace 6](#_Toc536695790)

[3 Náklady a pracnosti 7](#_Toc536695791)

[3.1 Přímé výdaje na realizaci záměrů 7](#_Toc536695792)

[3.2 Odhad výdajů na udržitelnost záměrů 9](#_Toc536695793)

[3.3 Pracnosti realizace záměrů 10](#_Toc536695794)

[4 Postupy řízení realizace cílů 10](#_Toc536695796)

[4.1 Přehled pokrytí dílčích cílů záměry 10](#_Toc536695797)

[4.2 Přehled záměrů v členění podle gesčních úřadů 11](#_Toc536695798)

[5 Matice odpovědností 11](#_Toc536695799)

[6 Příloha – Přehled záměrů klasifikace A dle cílů 12](#_Toc536695800)

# Základní informace o implementačním plánu

## Rekapitulace dílčích cílů implementačního plánu

Bezpečnost v internetovém prostředí je klíčová pro dobré fungování digitalizované společnosti s důvěrou občanů a organizací. Jedná se, jak o obranu proti kybernetickým útokům a zajištění efektivní a kvalitní kybernetické infrastruktury, tak o ochranu soukromí a osobních i obchodních údajů uživatelů. Tuto důvěru a bezpečnost je nutné stejnou měrou zajistit napříč všemi sektory, vertikálami digitální ekonomiky. K tomu je potřebné zejména celostní porozumění všem rizikům a hrozbám a koordinovaný vývoj a aplikace odpovídajících opatření, obvykle kombinací právní regulace, technických opatření, vzdělávání a výchovy. Přehled dílčích cílů je znázorněn v tabulce.

|  |  |  |
| --- | --- | --- |
| Dílčí cíl | Název | Popis |
| DES 5.01 | DES 5.01 Podpora opatření kybernetické bezpečnosti pro veřejnou správu. | Podpora opatření kybernetické bezpečnosti pro veřejnou správu.  • Vytvoření mechanismu spolupráce na národní úrovni mezi jednotlivými subjekty kybernetické bezpečnosti (pracoviště typu CERT a CSIRT) a posílení jejich stávajících struktur. Podpora vzniku dalších pracovišť typu CERT a CSIRT v ČR, - součástí platného Akčního plánu ke Strategii kybernetické bezpečnosti 2015-2020 (dále AP KB 2015-2020),  • poskytování služeb GovCERT veřejným institucím, subjektům kritické informační infrastruktury a subjektům systémů základní služby - součástí AP KB 2015-2020, • navyšování integrity sítí kritické informační infrastruktury – součástí AP KB 2015-2020,  • zajištění lepší a efektivnější spolupráce s GovCERT a jinými státními orgány – součástí AP KB 2015-2020, • Vytvoření záložních scénářů fungování společnosti, například v důsledku výpadku v elektrické síti nebo kybernetického útoku – součástí AP KB 2015-2020, • Zřízení nezávislého znaleckého a standardizačního centra, které by umožnilo objektivně hodnotit bezpečnost jednotlivých prvků kritické informační infrastruktury (KII). - součástí AP KB 2015-2020. |
| DES 5.02 | DES 5.02 Spolupráce se soukromým sektorem. | Spolupráce se soukromým sektorem.  • Vytvoření platformy pro sdílení informací o kybernetických hrozbách, incidentech a aktuálních zranitelnostech. Vytváření jednotných bezpečnostních norem. Např. aplikace vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti, která je jako standard uplatnitelná jak pro orgány veřejné správy, tak i soukromé – nepovinné – subjekty, součástí AP KB 2015-2020, • rozvíjení kontaktů a spolupráce se soukromým sektorem a zvyšování povědomí o činnosti a možnostech spolupráce s NÚKIB v oblasti kybernetické bezpečnosti prostřednictvím pravidelných jednání a vzájemného sdílení informací – součástí AP KB 2015-2020,  • osvěta, metodika a sdílení příkladů dobré praxe – součástí AP KB 2015-2020,  • bezpečnost a otázka zajištění bezpečnosti a spolehlivosti finančních transakcí a jejich digitalizace, • podpora koordinace a podílení se na projektech výzkumu a vývoji v oblasti kybernetické bezpečnosti – stát jako zadavatel vývoje bezpečnostních technologií,  • zajistit provoz národního koordinačního centra podle nařízení Evropského parlamentu a Rady o Evropském průmyslovém, technologickém a výzkumném centru kompetencí pro kybernetickou bezpečnost a síti národních koordinačních center. |
| DES 5.03 | DES 5.03 Osvěta široké veřejnosti a rozvoj lidského kapitálu. | Osvěta široké veřejnosti a rozvoj lidského kapitálu. NÚKIB ve spolupráci s institucionálními partnery a v souladu s úkoly uloženými vládou v AP KB bude pracovat na navyšování povědomí a gramotnosti v otázkách kybernetické bezpečnosti jak u dětí a pedagogů, tak u široké veřejnosti, resp. u všech koncových uživatelů. Opatření plánovaná za tímto účelem, zahrnují mimo jiné:  • Vytvoření e-learningové platformy pro vzdělávání širší a odborné veřejnosti (zejména dostupnost na principu otevřené univerzity),  • vytvoření metodických materiálů a doporučení pro školy pro zapracování kybernetické bezpečnosti do školních vzdělávacích programů – ve spolupráci s MŠMT, • prvek kybernetické bezpečnosti jako nezbytné součásti digitálního vzdělávání a digitální gramotnosti – ve spolupráci s MŠMT a MPSV – součástí AP KB 2015-2020, • podporu iniciativ a osvětových kampaní, pořádání osvětových akcí pro veřejnost, resp. koncové uživatele ve spolupráci s MPSV,  • podporu studijních programů pro výchovu expertů na kybernetickou bezpečnost vč. vysokoškolských stáží v oblasti kybernetické bezpečnosti v ČR i zahraničí – ve spolupráci s vysokými školami. |
| DES 5.05 | DES 5.05 Vytvoření záložních scénářů fungování společnosti, například v důsledku výpadku v elektrické síti nebo kybernetického útoku. | Vytvoření záložních scénářů fungování společnosti, například v důsledku výpadku v elektrické síti nebo kybernetického útoku. Naplnění tohoto cíle je myšleno pro všechny součásti digitální ekonomiky, která bude na elektrické energii a digitální konektivitě závislá. Řešit otázky energetické a kybernetické bezpečnosti, ale na druhou stranu je stále třeba učit všechny složky společnosti fungovat (po nějakou dobu) i bez elektřiny a bez digitálních informací. Prakticky by se to mělo stát součástí výuky i výcviku civilní ochrany obyvatelstva. Součástí AP KB 2015-2020. |

*Poznámka:*

*AP KB 2015-2020 = Akčního plánu kybernetické bezpečnosti 2015-2020*

## Klasifikace záměrů A, B a C

A. Záměr je dlouhodobě připravený, schválený v gesčním úřadu, je „v běhu“, má zajištěné financování (např. projekty již schválené OHA). V rámci metodiky to odpovídá stavu „závazku“, popř. dalších stavů. Záměry „A“ jsou uvedeny v příloze implementačního plánu.

B. Záměr je definovaný gesčním úřadem, tj. má prioritu a podporu v gesčním úřadu, ale nemá finanční nebo personální krytí. Tyto záměry tvoří těžiště implementačního plánu.

C. Potřebný záměr, existuje koncept záměru (tj. prakticky všechny políčka jsou vyplněná), ale není dojednána podpora gestora gesční úřad, ani zdroje (typicky průřezové záměry, multirezortní a sdílené).

V katalogu záměrů se nachází ještě další záměry ve stavu „**D**“, tj. námět na záměr. Tyto náměty vznikly z různých inspirací, například z potřeby pomoci úřadům dostát požadavkům architektonických principů a zásad řízení ICT ze schválené Informační koncepce. Mnohé náměty mohou být ještě duplicitní nebo příliš detailní, proto je pro jejich převod do stavu „C“ při příštím implementačním plánování nutná jejich konsolidace.

## Shrnutí problematiky, celkové přínosy

**Zajištění bezpečnosti a důvěry v prostředí digitální ekonomiky a společnosti**

Rozmach v oblasti digitální ekonomiky je spojen s kybernetickými hrozbami a riziky. Ke správnému fungování digitální ekonomiky je nezbytná kybernetická bezpečnost. K tomu, aby digitalizovaná společnost dobře fungovala, a aby v ni organizace i občané měli důvěru, je klíčové zajistit bezpečnost v internetovém prostředí. Požadavkem je vysoká digitální důvěra všech stran v digitální prostor. Jedná se, jak o obranu proti kybernetickým útokům a zajištění efektivní a kvalitní kybernetické infrastruktury, tak o ochranu soukromí a osobních i obchodních údajů uživatelů.

Soukromí a bezpečnost je ústředním bodem budování důvěry na internetu a v digitální ekonomice. S rostoucím počtem digitálních služeb a úrovní rizika roste potřeba posílení důvěry a bezpečnosti prostředí pro využívání informačních a komunikačních technologií jako základ pro hospodářský růst a prosperitu. Bezpečná kybernetická infrastruktura tvoří nezbytnou podmínku pro rozvoj digitální ekonomiky.

*Vize ČR v oblasti kybernetické bezpečnosti jsou obsaženy v Národní strategii kybernetické bezpečnosti na období let 2015-2020 a v navazujícím Akčním plánu.*

## Souhrnné údaje

Statistika katalogu záměrů dle stupně připravenosti (A, B, C).

### Počty záměrů a odhad finanční alokace v rezortech a úřadech (klasifikace A, B, C)

|  |  |  |  |
| --- | --- | --- | --- |
| **Gesční úřad** | **Počet záměrů** | **Externí náklady realizace od (mil. Kč)** | **Externí náklady realizace do (mil. Kč)** |
| **A** |  |  |  |
| NÚKIB | 14 | 335,000 | 335,000 |
| **B** |  |  |  |
| NÚKIB | 1 | 30,000 | 30,000 |
| **Celkový součet** | **15** | **365,000** | **365,000** |

### Počty záměrů a odhad finanční alokace v dílčích cílech (klasifikace A, B, C)

|  |  |  |  |
| --- | --- | --- | --- |
| **Dílčí cíl** | **Počet záměrů** | **Externí náklady realizace od (mil. Kč)** | **Externí náklady realizace do (mil. Kč)** |
| **A** |  |  |  |
| DES 5.01 | 8 | 0,000 | 0,000 |
| DES 5.02 | 2 | 0,000 | 0,000 |
| DES 5.03 | 2 | 335,000 | 335,000 |
| DES 5.04 | 1 | 0,000 | 0,000 |
| DES 5.05 | 1 | 0,000 | 0,000 |
| **B** |  |  |  |
| DES 5.02 | 1 | 30,000 | 30,000 |
| **Celkový součet** | **15** | **365,000** | **365,000** |

# Sestava záměrů dle data ukončení realizace

|  |  |
| --- | --- |
| **Rok realizace do / Název záměru** | **Počet záměrů** |
| **2020** |  |
| **Čtv1** |  |
| Navyšování integrity sítí kritické informační infrastruktury – součástí AP KB 2015-2020 | 1 |
| Podporu iniciativ a osvětových kampaní, pořádání osvětových akcí pro veřejnost, resp. koncové uživatele ve spolupráci s MPSV – součástí AP KB 2015-2020 | 1 |
| Poskytování služeb GovCERT veřejným institucím, subjektům kritické informační infrastruktury a subjektům systémů základní služby - součástí AP KB 2015-2020 | 1 |
| Prvek kybernetické bezpečnosti jako nezbytné součásti digitálního vzdělávání a digitální gramotnosti – ve spolupráci s MŠMT a MPSV – součástí AP KB 2015-2020 | 1 |
| Rozvíjení kontaktů a spolupráce se soukromým sektorem a zvyšování povědomí o činnosti a možnostech spolupráce s NÚKIB v oblasti kybernetické bezpečnosti prostřednictvím pravidelných jednání a vzájemného sdílení informací. - součástí AP KB 2015-2020 | 1 |
| **Splnění Akčního plánu kybernetické bezpečnosti 2015–2020** | **1** |
| Vytvoření mechanismu spolupráce na národní úrovni mezi jednotlivými subjekty kybernetické bezpečnosti (pracoviště typu CERT a CSIRT) a posílení jejich stávajících struktur. Podpora vzniku dalších pracovišť typu CERT a CSIRT v ČR - součástí AP KB 2015-2020 | 1 |
| Vytvoření platformy pro sdílení informací o kybernetických hrozbách, incidentech a aktuálních zranitelnostech. Vytváření jednotných bezpečnostních norem. Např. aplikace vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti, která je jako standard uplatnitelná jak pro orgány veřejné správy, tak i soukromé – nepovinné – subjekty - součástí AP KB 2015-2020 | 1 |
| Zajištění lepší a efektivnější spolupráce s GovCERT a jinými státními orgány - součástí AP KB 2015-2020 | 1 |
| Vytvoření záložních scénářů fungování společnosti - součástí AP KB 2015-2020 | 1 |
| Zřízení nezávislého znaleckého a standardizačního centra, které by umožnilo objektivně hodnotit bezpečnost jednotlivých prvků kritické informační infrastruktury (KII) - součástí AP KB 2015-2020 | 1 |
| **2022** |  |
| **Čtv4** |  |
| Zajistit provoz národního koordinačního centra podle nařízení Evropského parlamentu a Rady o Evropském průmyslovém, technologickém a výzkumném centru kompetencí pro kybernetickou bezpečnost a síti národních koordinačních center | 1 |
| Vytvoření záložních scénářů fungování společnosti – součástí AP KB 2015-2020 | 1 |
| **Celkový součet** | **13** |

*Poznámka:*

*AP KB 2015-2020 = Akčního plánu kybernetické bezpečnosti 2015-2020*

# Náklady a pracnosti

## Přímé výdaje na realizaci záměrů

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Název** | **Stav** | **Realizace od** | **Realizace do** | **Dílčí cíl** | **Celkový dopad** | **Celková náročnost** | **Gesční úřad záměru** | **Externí náklady realizace do (mil. Kč)** |
| Vytvoření mechanismu spolupráce na národní úrovni mezi jednotlivými subjekty kybernetické bezpečnosti (pracoviště typu CERT a CSIRT) a posílení jejich stávajících struktur. Podpora vzniku dalších pracovišť typu CERT a CSIRT v ČR | A | 01.01.2015 | 01.01.2020 | DES 5.01 | 3 | 3 | NÚKIB |  |
| Školení zaměstnanců státní správy v oblasti kybernetické bezpečnosti | A | 01.01.2015 | 01.01.2020 | DES 5.01 | 3 | 3 | NÚKIB |  |
| Zajištění lepší a efektivnější spolupráce s GovCERT a jinými státními orgány | A | 01.01.2015 | 01.01.2020 | DES 5.01 | 3 | 2 | NÚKIB |  |
| Poskytování služeb GovCERT veřejným institucím, subjektům kritické informační infrastruktury a subjektům systémů základní služby - součástí AP KB 2015-2020 | A | 01.01.2015 | 01.01.2020 | DES 5.01 | 4 | 4 | NÚKIB |  |
| Navyšování integrity sítí kritické informační infrastruktury | A | 01.01.2015 | 01.01.2020 | DES 5.01 | 4 | 4 | NÚKIB |  |
| Splnění Akčního plánu kybernetické bezpečnosti 2015 - 2020 | A | 01.01.2015 | 01.01.2020 | DES 5.01 | 5 | 4 | NÚKIB |  |
| Zřízení nezávislého znaleckého a standardizačního centra, které by umožnilo objektivně hodnotit bezpečnost jednotlivých prvků kritické informační infrastruktury (KII) | A | 01.01.2015 | 01.01.2020 | DES 5.01 | 4 | 5 | NÚKIB |  |
| Vytvoření platformy pro sdílení informací o kybernetických hrozbách, incidentech a aktuálních zranitelnostech. Vytváření jednotných bezpečnostních norem; Např. aplikace vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti, která je jako standard uplatnitelná jak pro orgány veřejné správy, tak i soukromé – nepovinné – subjekty | A | 01.01.2015 | 01.01.2020 | DES 5.02 | 3 | 3 | NÚKIB |  |
| Rozvíjení kontaktů a spolupráce se soukromým sektorem a zvyšování povědomí o činnosti a možnostech spolupráce s NÚKIB v oblasti kybernetické bezpečnosti prostřednictvím pravidelných jednání a vzájemného sdílení informací | A | 01.01.2015 | 01.01.2020 | DES 5.02 | 3 | 3 | NÚKIB |  |
| Podporu iniciativ a osvětových kampaní, pořádání osvětových akcí pro veřejnost, resp. koncové uživatele ve spolupráci s MPSV - součástí AP KB 2015-2020 | A | 01.01.2015 | 01.01.2020 | DES 5.03 | 3 | 2 | NÚKIB | 335 |
| Prvek kybernetické bezpečnosti jako nezbytné součásti digitálního vzdělávání a digitální gramotnosti – ve spolupráci s MŠMT a MPSV - součástí AP KB 2015-2020 | A | 01.01.2015 | 01.01.2020 | DES 5.03 | 4 | 3 | NÚKIB |  |
| Zajistit provoz národního koordinačního centra podle nařízení Evropského parlamentu a Rady o Evropském průmyslovém, technologickém a výzkumném centru kompetencí pro kybernetickou bezpečnost a síti národních koordinačních center | B | 01. 06. 2019 | 01. 06. 2020 | DES 5.02 | 3 | 3 | NÚKIB | 30 |
| Zajištění souběžných záložních scénářů fungování společnosti | B | 01.01.2019 | 01.01.2022 | DES 5.05 | 4 | 2 | Vlastníci poskytovatelů zdravotních služeb | 2000 |
| Vytvoření záložních scénářů fungování společnosti | A | 01.01.2015 | 01.01.2020 | DES 5.05 | 3 | 3 | NÚKIB |  |

*Poznámka:*

*AP KB 2015-2020 = Akčního plánu kybernetické bezpečnosti 2015-2020*

## Odhad výdajů na udržitelnost záměrů

Vládní program Digitální Česko, strategický průřezový dokument, zastřešuje tři hlavní, do značné míry rozdílné pilíře. Postup naplňování cílů jednotlivých koncepcí bude mít, vzhledem ke specifičnosti koncepcí, rozdílný charakter. Postupy z jednoho z nich nelze aplikovat na zbývající dokumenty, které mají odlišnou povahu. Koncepce Digitální ekonomika a společnost (DES), svěřená do gesce Ministerstva průmyslu a obchodu (MPO) má naprosto specifický, vysoce meziresortní a mezioborový charakter.

Koncepce DES je komplexním strategickým dokumentem s primárním zaměřením na národní strategie a přesahem na klíčové iniciativy v EU. Navazuje přitom na Akční plán pro společnost 4.0 a další dřívější vládní strategie, stejně jako dokumenty Evropské unie. Jednotlivé Implementační plány Koncepce Digitální ekonomika a společnost, které identifikují zásadní oblasti pro rozvoj digitální ekonomiky, jsou výsledkem meziresortní spolupráce, odborné veřejnosti i zástupců hospodářských a sociálních partnerů.

Účelem koncepce DES je zajistit koordinaci agend spadajících do různých oblastí digitální ekonomiky a života společnosti napříč veřejnou správou, hospodářskými a sociálními partnery, akademickou sférou a odbornou veřejností, shrnout a průběžně aktualizovat klíčová opatření vlády na podporu rozvoje digitálního trhu a digitální ekonomiky České republiky v souladu s předpisy EU.

Základním cílem Implementačních plánů koncepce DES je prostřednictvím navrhovaných výstupů zvýšit připravenost ČR na digitální ekonomiku, zlepšit transfer výsledků výzkumu do praxe a maximalizovat hospodářský potenciál země. Jednotlivé záměry mohou mít podobu projektu, akčního plánu nebo jiného konkrétního výstupu (služba, systém, regulační akt, analýza, resortní strategie, návrhy legislativy apod.).

Zajištění bezpečnosti a důvěry v prostředí digitální ekonomiky a společnosti je v současné době citováno na všech úrovních jak v ČR, tak v mezinárodním měřítku. Záměry uvedené v tomto dílčím cíli jsou specifické pro své cílové skupiny i způsoby naplnění a není v současné době možné na centrální úrovni určit odhady výdajů na udržitelnost záměrů. Nejsou k dispozici ukazatele sledování nákladů na udržitelnost jednotlivých záměrů ve státní správě. Plnění cílů navíc ovlivňují i směrnice EU.

## Pracnosti realizace záměrů

Česká republika podporuje iniciativy zaměřené na další ekonomický růst a vytváření příznivého digitálního ekosystému. Hlavním cílem při přípravě Implementačních plánů DES bylo získat jasný a ucelený přehled o klíčových aktivitách relevantních ústředních orgánů státní správy, hospodářských i sociálních partnerů a zástupců byznysu a akademické sféry. Klíčem k úspěchu je efektivní komunikace a spolupráce napříč resorty, podnikovou a vědeckou sférou i odbornou veřejností tak, aby se jasně určily klíčové priority s přímou návazností na programové prohlášení vlády, které jsou mimořádně důležité pro vývoj digitální ekonomiky a zvyšování konkurenceschopnosti ČR.

**S ohledem na meziresortní a mezioborový charakter dílčího cíle zajištění bezpečnosti a důvěry v prostředí digitální ekonomiky a společnosti není možné měřit pracnost realizace záměrů v rámci veřejné správy na centrální úrovni. Naplňování jednotlivých cílů má úzkou návaznost na projednávání legislativních i nelegislativních iniciativ Evropské unie, včetně příslušných výstupů Rady EU, a rovněž i na rozdělení gescí a kompetencí jednotlivých resortů v souladu s kompetenčním zákonem. Na úrovni jednotlivých resortů napříč veřejnou správou není v současné době měření nákladovosti a efektivity dostupné.**

# Postupy řízení realizace cílů

## Přehled pokrytí dílčích cílů záměry

|  |  |  |  |
| --- | --- | --- | --- |
| **Gesční úřad / Název záměru/ Popis záměru** | **DES 5.02** | **DES 5.05** | **Celkový součet** |
| Zajistit provoz národního koordinačního centra podle nařízení Evropského parlamentu a Rady o Evropském průmyslovém, technologickém a výzkumném centru kompetencí pro kybernetickou bezpečnost a síti národních koordinačních center. |  |  |  |
| **Vytvoření záložních scénářů fungování společnosti** | **1** | **2** | **2** |
| Zajištění finančních prostředků pro poskytovatele zdravotních služeb. Ochrana kritických služeb státu při zajištění zdravotních služeb.  Aplikace bezpečnostních opatření a technologií pro ochranu před kybernetickými útoky majících za dopad ohrožení obyvatelstva. |  |  |  |
| **Celkový součet** | **1** | **2** | **3** |

## Přehled záměrů v členění podle gesčních úřadů

|  |  |
| --- | --- |
| **Gesční úřad / Název záměru / Spolupracující úřady** | **Počet záměrů** |
| **NÚKIB** | **1** |
| MV; NAKIT | 1 |
| **Celkový součet** | **2** |

# Matice odpovědností

|  |  |  |  |
| --- | --- | --- | --- |
| Gesční úřad / Název záměru | prof. MUDr. Roman Prymula, CSc., Ph.D./  Ing. Jiří Borej | Viktor Paggio (NUKIB) | Celkový součet |
| NÚKIB |  |  |  |
| Vlastníci poskytovatelů zdravotních služeb | 2 |  | 2 |
| Zajistit provoz národního koordinačního centra kybernetické bezpečnosti podle nařízení Evropského parlamentu a Rady |  | 1 |  |
| Zajištění souběžných záložních scénářů fungování společnosti | 2 |  | 2 |
| Celkový součet | 4 | 1 | 5 |

# Příloha – Přehled záměrů klasifikace A dle cílů

|  |  |
| --- | --- |
| Gesční úřad / Název záměru / Popis záměru / Výstup záměru | Počet záměrů |
| NÚKIB | 27 |
| Zahájení společného projektu „Trojúhelník kybernetické bezpečnosti ČR“ | 1 |
| Navyšování integrity sítí kritické informační infrastruktury | 1 |
| Na již několika prvcích KII určuje zákon o kyber. bezpečnosti a navazující vyhláška, NÚKIB poskytuje subjektům metodickou podporu a provádí státní dozor | 1 |
| Poskytování metodické podpory a státní dozor | 1 |
| Podporu iniciativ a osvětových kampaní, pořádání osvětových akcí pro veřejnost, resp. koncové uživatele ve spolupráci s MPSV - součástí AP KB 2015-2020 | 1 |
| Podpora základní znalosti pravidel kybernetické bezpečnosti a zapojení neziskových osvětových organizací působících v oblasti kybernetické bezpečnosti a prevence rizik souvisejících s užíváním prostředků ICT a internetu | 1 |
| Poskytování služeb GovCERT veřejným institucím, subjektům kritické informační infrastruktury a subjektům systémů základní služby, - součástí AP KB 2015-2020 | 1 |
| Vládní CERT České republiky (GovCERT.CZ) kontinuálně poskytuje široké spektrum služeb veřejným institucím, subjektům kritické informační infrastruktury a subjektům systémů základní služby | 1 |
| Prvek kybernetické bezpečnosti jako nezbytné součásti digitálního vzdělávání a digitální gramotnosti – ve spolupráci s MŠMT a MPSV – součástí AP KB 2015-2020 | 1 |
| Zajistit provoz národního koordinačního centra podle nařízení Evropského parlamentu a Rady o Evropském průmyslovém, technologickém a výzkumném centru kompetencí pro kybernetickou bezpečnost a síti národních koordinačních center | 1 |
| Zajištění dostupného poradenství v otázkách bezpečnosti a příležitostí včetně internetového poradenství Komunikační aktivity pro veřejnost.  Komunikační a vzdělávací aktivity pro úředníky/zaměstnance veřejné správy směřující ke znalosti nástrojů eGovernmentu a znalosti bezpečného používání prostředků ICT a internetu včetně dopadů Zákona o kybernetické bezpečnosti | 1 |
| Rozvíjení kontaktů a spolupráce se soukromým sektorem a zvyšování povědomí o činnosti a možnostech spolupráce s NÚKIB v oblasti kybernetické bezpečnosti prostřednictvím pravidelných jednání a vzájemného sdílení informací | 1 |
| Každoroční pořádání konference kybernetické bezpečnosti CyberCon Brno pro širokou veřejnost, semináře k ZKB a dalších osvětových akcí nejen pro subjekty soukromého sektoru | 1 |
| Splnění Akčního plánu kybernetické bezpečnosti 2015–2020 | 1 |
| **Splnění všech úkolů vyjmenovaných v Akčním plánu k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020** Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020 schválila Vláda České republiky 25. května 2015, Akční plán je dlouhodobě realizován a pro vládu pravidelně jednou ročně vyhodnocován. | 1 |
| Hlavní výstupy:  splněné body Akčního plánu ve všech definovaných oblastech, tj.  ● Zajištění efektivity a posilování všech struktur, procesů a spolupráce při zajišťování kybernetické bezpečnosti  ● Aktivní mezinárodní spolupráce  ● Ochrana národní KII a VIS  ● Spolupráce se soukromým sektorem  ● Výzkum a vývoj / spotřebitelská důvěra  ● Podpora vzdělávání, osvěta a rozvoj informační společnosti  ● Podpora rozvoje schopností PČR vyšetřovat a postihovat informační kriminalitu  ● Právní úprava pro kybernetickou bezpečnost (vytváření právního rámce), účast na tvorbě a implementaci evropských a mezinárodních pravidel | 1 |
| Školení zaměstnanců státní správy v oblasti kybernetické bezpečnosti | 1 |
| Vytvoření mechanismu spolupráce na národní úrovni mezi jednotlivými subjekty kybernetické bezpečnosti (pracoviště typu CERT a CSIRT) a posílení jejich stávajících struktur. Podpora vzniku dalších pracovišť typu CERT a CSIRT v ČR | 1 |
| Naplňování Akčního plánu a Národní strategii kybernetické bezpečnosti České republiky na období let 2015–2020 | 1 |
| Vytvoření platformy pro sdílení informací o kybernetických hrozbách, incidentech a aktuálních zranitelnostech. Vytváření jednotných bezpečnostních norem. Např. aplikace vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti, která je jako standard uplatnitelná jak pro orgány veřejné správy, tak i soukromé – nepovinné – subjekty. | 1 |
| Informace o kybernetických hrozbách, incidentech a aktuálních zranitelnostech NÚKIB pravidelně zveřejňuje na svých webových stránkách, případě twitterovém účtu. Zároveň se finalizuje projekt "neveřejného webu" pro efektivnější a důvěrnější sdílení těchto informací s povinnými subjekty dle ZKB. | 1 |
| Pravidelné zveřejňování informací o kybernetických hrozbách, incidentech a aktuálních zranitelnostech na webových stránkách NUKIB, případě twitterovém účtu, finalizace projektu "neveřejného webu" pro efektivnější a důvěrnější sdílení těchto informací s povinnými subjekty dle ZKB. | 1 |
| Zajištění lepší a efektivnější spolupráce s GovCERT a jinými státními orgány | 1 |
| Spolupráce kontinuálně prováděná a zlepšována. Zároveň je průběžně vyhodnocována v každoroční Zprávě o stavu kybernetické bezpečnosti ČR. | 1 |
| Kontinuální provádění a zlepšování spolupráce s GovCERT a jinými státními orgány a průběžné vyhodnocování v každoroční Zprávě o stavu kybernetické bezpečnosti ČR | 1 |
| Vytvoření záložních scénářů fungování společnosti | 1 |
| Zřízení nezávislého znaleckého a standardizačního centra, které by umožnilo objektivně hodnotit bezpečnost jednotlivých prvků kritické informační infrastruktury (KII). | 1 |
| Celkový součet | 27 |