digitální ; ČESKO

Vládní program digitalizace
České republiky 2018+

DIGITÁLNÍ EKONOMIKA A SPOLEČNOST

Implementační plán hlavního cíle č. 5 - DES
IP Zajištění bezpečnosti a důvěry v prostředí digitální ekonomiky a společnosti

Verze dokumentu: **1.2**

Datum poslední změny dokumentu: **27. 3. 2019**

Poznámka k verzi:

připomínky NÚKIB zapracovány 25. 1. 2019

Úřad vlády České republiky, Nábřeží Edvarda Beneše 4, 118 01 Malá Strana
info@digitalnicesko.cz digitalnicesko.cz

Obsah

1 Základní informace o implementačním plánu

1.1 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 odolnost vůči 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.

Název dílčího cíle	Popis dílčího cíle
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 **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.

Název dílčího cíle	Popis dílčího cíle
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 **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

1.2 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.

1.3 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.

1.4 Souhrnné údaje (záměry A, B, C)

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

1.4.1 Počty záměrů a odhad finanční alokace v rezortech a úřadech

Stav / Gesční úřad	Počet záměrů	Externí náklady realizace od (mil. Kč)	Externí náklady realizace do (mil. Kč)
A	**13**	**335,00**	**335,00**
NÚKIB	13	335,00	335,00
C	**1**	**250,00**	**250,00**
NÚKIB	1	250,00	250,00
Celkový součet	**14**	**585,00**	**585,00**

1.4.2 Počty záměrů a odhad finanční alokace v dílčích cílech

Stav / Dílčí cíl	Počet záměrů	Externí náklady realizace od (mil. Kč)	Externí náklady realizace do (mil. Kč)
A	**13**	**335,00**	**335,00**
DES 5.01	8	0,00	0,00
DES 5.02	2	0,00	0,00
DES 5.03	1	335,00	335,00
DES 5.04	1	0,00	0,00
DES 5.05	1	0,00	0,00
C	**1**	**250,00**	**250,00**
DES 5.01	1	250,00	250,00
Celkový součet	**14**	**585,00**	**585,00**

2 Sestava záměrů dle data ukončení realizace (záměry A, B, C)

Rok realizace (do) / Měsíc realizace / Název záměru	Počet záměrů	Součet z Exter. náklady realizace od (mil. Kč)	Součet z Exter. náklady realizace do (mil. Kč)
2020	**14**	**585,00**	**585,00**
1	**13**	**335,00**	**335,00**
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	0,00	0,00
Na základě vyhodnocování světových trendů v rozvoji kybernetické bezpečnosti navrhnout a zahájit společný projekt „Trojúhelník kybernetické bezpečnosti ČR“	1	0,00	0,00
Školení zaměstnanců státní správy v oblasti kybernetické bezpečnosti	1	0,00	0,00
Zajištění lepší a efektivnější spolupráce s GovCERT a jinými státními orgány.	1	0,00	0,00
Poskytování služeb GovCERT veřejným institucím, subjektům kritické informační infrastruktury a subjektům systémů základní služby,	1	0,00	0,00
Navyšování integrity sítí kritické informační infrastruktury	1	0,00	0,00
Splnění Akčního plánu kybernetické bezpečnosti 2015–2020	1	0,00	0,00
Zřízení nezávislého znaleckého a standardizačního centra (KII)	1	0,00	0,00
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	0,00	0,00
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	0,00	0,00
Podporu iniciativ a osvětových kampaní, pořádání osvětových akcí pro veřejnost, resp. koncové uživatele ve spolupráci s MPSV	1	335,00	335,00
Zajištění zálohování napájení kritických uzlů a zařízení	1	0,00	0,00
Souběžné záložní scénáře fungování společnosti – AP KB 2015-2020	1	0,00	0,00
12	**1**	**250,00**	**250,00**
Masivní eLearning zaměřený kybernetickou bezpečnost pro veřejnou správu	1	250,00	250,00
Celkový součet	**14**	**585,00**	**585,00**

Poznámka:

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

3 Náklady a pracnosti (záměry A, B, C)

3.1 Přímé výdaje na realizaci záměrů

Název	Stav	Realizace od	Realizace do	Dílčí cíl	Gesční úřad záměru	Exter. náklady realizace od (mil. Kč)	Exter. 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	NÚKIB		
Na základě vyhodnocování světových trendů v rozvoji kybernetické bezpečnosti navrhnout a zahájit společný projekt „Trojúhelník kybernetické bezpečnosti ČR“	A	01.01.2015	01.01.2020	DES 5.01	NÚKIB		
Školení zaměstnanců státní správy v oblasti kybernetické bezpečnosti	A	01.01.2015	01.01.2020	DES 5.01	NÚKIB		
Zajištění lepší a efektivnější spolupráce s GovCERT a jinými státními orgány.	A	01.01.2015	01.01.2020	DES 5.01	NÚKIB		
Masivní elearning zaměřený kybernetickou bezpečnost pro veřejnou správu	C	01.01.2015	31.12.2020	DES 5.01	NÚKIB	250	250
Poskytování služeb GovCERT veřejným institucím, subjektům kritické informační infrastruktury a subjektům systémů základní služby,	A	01.01.2015	01.01.2020	DES 5.01	NÚKIB		
Navyšování integrity sítí kritické informační infrastruktury	A	01.01.2015	01.01.2020	DES 5.01	NÚKIB		
Splnění Akčního plánu kybernetické bezpečnosti 2015–2020	A	01.01.2015	01.01.2020	DES 5.01	NÚKIB		

Název	Stav	Realizace od	Realizace do	Dílčí cíl	Gesční úřad záměru	Exter. náklady realizace od (mil. Kč)	Exter. náklady realizace do (mil. Kč)
Zřízení nezávislého znaleckého a standardizačního centra (KII)	A	01.01.2015	01.01.2020	DES 5.01	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	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	NÚKIB		
Podporu iniciativ a osvětových kampaní, pořádání osvětových akcí pro veřejnost, resp. koncové uživatele ve spolupráci s MPSV	A	01.01.2015	01.01.2020	DES 5.03	NÚKIB	335	335
Zajištění zálohování napájení kritických uzlů a zařízení	A	01.01.2015	01.01.2020	DES 5.04	NÚKIB		
Souběžné záložní scénáře fungování společnosti – AP KB 2015-2020	A	01.01.2015	01.01.2020	DES 5.05	NÚKIB		

Poznámka:

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

3.2 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 právní akty EU.

3.3 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.

4 Postupy řízení realizace (záměry A,B,C)

4.1 Přehled pokrytí dílčích cílů záměry

Gesční úřad / Název záměru / Popis záměru	DES 5.01	DES 5.02	DES 5.03	DES 5.04	DES 5.05	Celkový součet
NÚKIB	**9**	**2**	**1**	**1**	**1**	**14**
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**					**1**
Popsán v Akčním plánu a Národní strategii kybernetické bezpečnosti České republiky na období let 2015–2020.	1					1
Na základě vyhodnocování světových trendů v rozvoji kybernetické bezpečnosti navrhnout a zahájit společný projekt „Trojúhelník kybernetické bezpečnosti ČR“	**1**					**1**
Projekt bude realizován za úzké spolupráce mezi Národním úřadem pro kybernetickou a informační bezpečnost, Ministerstvem obrany (Cyber Defence) a Ministerstvem vnitra (dohledové centrum eGovernmentu).	1					1
Školení zaměstnanců státní správy v oblasti kybernetické bezpečnosti	**1**					**1**
E-learningové kurzy kybernetické bezpečnosti pro vybrané cílové skupiny – úředníky a manažery kybernetické bezpečnosti.	1					1
Zajištění lepší a efektivnější spolupráce s GovCERT a jinými státními orgány	**1**					**1**
Spolupráce kontinuálně prováděná a zlepšována. Zároveň je průběžně vyhodnocována v každoroční Zprávě o stavu kybernetické bezpečnosti ČR.	1					1
Masivní elearning zaměřený kybernetickou bezpečnost pro veřejnou správu	**1**					**1**
2letý intenzivní elearning zaměřený na základní kybernetickou hygienu spojený s anti-phishingovými testy pro úředníky státní správy, samosprávy a podniků s většinovou veřejnou účastí. Záměr je již definovaný, obsah elearningu připravený, má prioritu, možná spolupráce více gestorů – zejména NÚKIB a MV, ale nemá personální a finanční krytí.	1					1
Poskytování služeb GovCERT veřejným institucím, subjektům kritické informační infrastruktury a subjektům systémů základní služby	**1**					**1**
Vládní CERT České republiky (GovCERT.CZ) kontinuálně poskytuje široké spektrum služeb veřejným institucím, subjektům kritické informační infrastruktury a subjektům systémů základní služby.	1					1
Navyšování integrity sítí kritické informační infrastruktury	**1**					**1**
NÚKIB poskytuje metodickou podporu všem subjektům kritické informační infrastruktury. Je určeno více než 100 prvků kritické informační infrastruktury.	1					1
Splnění Akčního plánu kybernetické bezpečnosti 2015–2020	**1**					**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					1

Gesční úřad / Název záměru / Popis záměru	DES 5.01	DES 5.02	DES 5.03	DES 5.04	DES 5.05	Celkový součet
Zřízení nezávislého znaleckého a standardizačního centra (KII)	**1**					**1**
Centrum by umožnilo objektivně hodnotit bezpečnost jednotlivých prvků kritické informační infrastruktury.	1					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**				**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				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**				**1**
Každoroční pořádání konference kybernetické bezpečnosti CyberCon Brno pro širokou veřejnost, semináře k ZKB a dalších osvětových akcí nejen pro subjekty soukromého sektoru		1				1
Podporu iniciativ a osvětových kampaní, pořádání osvětových akcí pro veřejnost, resp. koncové uživatele ve spolupráci s MPSV			**1**			**1**
			1			1
Zajištění zálohování napájení kritických uzlů a zařízení				**1**		**1**
Probíhající projekt podpory kybernetické bezpečnosti.				1		1
Souběžné záložní scénáře fungování společnosti – AP KB 2015-2020					**1**	**1**
Záměr je součástí schváleného Akčního plánu kybernetické bezpečnosti 2015-2020. Konkrétně ho v AP pokrývá sekce C „Ochrana národní KII a VIS“, bod C.10.02 „Definovat soubor možných krizových situací a vytvářet krizové scénáře pro spolupráci, komunikaci a nasazení protiopatření v období krizových stavů“ a C.10.03 „Provádět národní cvičení v oblasti komunikace, koordinace a spolupráce při zajišťování kybernetické obrany“.					1	1
Celkový součet	**9**	**2**	**1**	**1**	**1**	**14**

4.2 Přehled záměrů v členění podle gesčních úřadů

Gesční úřad / Název záměru / Spolupracující úřady	Počet záměrů
NÚKIB	**14**
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**
CERT; CSIRT	1
Na základě vyhodnocování světových trendů v rozvoji kybernetické bezpečnosti navrhnout a zahájit společný projekt „Trojúhelník kybernetické bezpečnosti ČR“	**1**
MO; MV	1
Školení zaměstnanců státní správy v oblasti kybernetické bezpečnosti	**1**
MV	1
Zajištění lepší a efektivnější spolupráce s GovCERT a jinými státními orgány.	**1**
MV	1
Masivní elearning zaměřený kybernetickou bezpečnost pro veřejnou správu	**1**
MV; NAKIT	1
Poskytování služeb GovCERT veřejným institucím, subjektům kritické informační infrastruktury a subjektům systémů základní služby,	**1**
MV	1
Navyšování integrity sítí kritické informační infrastruktury	**1**
MV	1
Splnění Akčního plánu kybernetické bezpečnosti 2015–2020	**1**
MV; MO; zpravodajské služby; MPO; MŠMT; MZV; další rezorty, CERT, CSIRT	1
Zřízení nezávislého znaleckého a standardizačního centra (KII)	**1**
MV	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**
MV	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**
MV	1
Podporu iniciativ a osvětových kampaní, pořádání osvětových akcí pro veřejnost, resp. koncové uživatele ve spolupráci s MPSV	**1**
ÚP ČR; MPSV	1
Zajištění zálohování napájení kritických uzlů a zařízení	**1**
MV	1
Souběžné záložní scénáře fungování společnosti – AP KB 2015-2020	**1**
MV	1
Celkový součet	**14**

5 Matice odpovědností (záměry A,B,C)

Název záměru	Viktor Paggio (NUKIB)/Roman Vrba (MV)	Viktor Paggio (NUKIB)	Celkový součet
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		1
Na základě vyhodnocování světových trendů v rozvoji kybernetické bezpečnosti navrhnout a zahájit společný projekt „Trojúhelník kybernetické bezpečnosti ČR“	1		1
Školení zaměstnanců státní správy v oblasti kybernetické bezpečnosti	1		1
Zajištění lepší a efektivnější spolupráce s GovCERT a jinými státními orgány.	1		1
Masivní elearning zaměřený kybernetickou bezpečnost pro veřejnou správu		1	1
Poskytování služeb GovCERT veřejným institucím, subjektům kritické informační infrastruktury a subjektům systémů základní služby,	1		1
Navyšování integrity sítí kritické informační infrastruktury	1		1
Splnění Akčního plánu kybernetické bezpečnosti 2015–2020		1	1
Zřízení nezávislého znaleckého a standardizačního centra (KII)	1		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		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		1
Podporu iniciativ a osvětových kampaní, pořádání osvětových akcí pro veřejnost, resp. koncové uživatele ve spolupráci s MPSV		1	1
Zajištění zálohování napájení kritických uzlů a zařízení	1		1
Souběžné záložní scénáře fungování společnosti – AP KB 2015-2020	1		1
Celkový součet	**11**	**3**	**14**

6 Příloha – Přehled záměrů klasifikace A

Gesční úřad / Název záměru / Popis záměru	Počet záměrů
NÚKIB	**13**
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**
Popsán v Akčním plánu a Národní strategii kybernetické bezpečnosti České republiky na období let 2015–2020.	1
Na základě vyhodnocování světových trendů v rozvoji kybernetické bezpečnosti navrhnout a zahájit společný projekt „Trojúhelník kybernetické bezpečnosti ČR“	**1**
Projekt bude realizován za úzké spolupráce mezi Národním úřadem pro kybernetickou a informační bezpečnost, Ministerstvem obrany (Cyber Defence) a Ministerstvem vnitra (dohledové centrum eGovernmentu).	1
Školení zaměstnanců státní správy v oblasti kybernetické bezpečnosti	**1**
E-learningové kurzy kybernetické bezpečnosti pro vybrané cílové skupiny – úředníky a manažery kybernetické bezpečnosti.	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
Poskytování služeb GovCERT veřejným institucím, subjektům kritické informační infrastruktury a subjektům systémů základní služby	**1**
Vládní CERT České republiky (GovCERT.CZ) kontinuálně poskytuje široké spektrum služeb veřejným institucím, subjektům kritické informační infrastruktury a subjektům systémů základní služby.	1
Navyšování integrity sítí kritické informační infrastruktury	**1**
NÚKIB poskytuje metodickou podporu všem subjektům kritické informační infrastruktury. Je určeno více než 100 prvků kritické informační infrastruktury.	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
Zřízení nezávislého znaleckého a standardizačního centra (KII)	**1**
Centrum by umožnilo objektivně hodnotit bezpečnost jednotlivých prvků kritické informační infrastruktury.	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
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

Gesční úřad / Název záměru / Popis záměru	Počet záměrů
Podporu iniciativ a osvětových kampaní, pořádání osvětových akcí pro veřejnost, resp. koncové uživatele ve spolupráci s MPSV	**1**
	1
Zajištění zálohování napájení kritických uzlů a zařízení	**1**
Probíhající projekt podpory kybernetické bezpečnosti.	1
Souběžné záložní scénáře fungování společnosti – AP KB 2015-2020	**1**
Záměr je součástí schváleného Akčního plánu kybernetické bezpečnosti 2015-2020. Konkrétně ho v AP pokrývá sekce C „Ochrana národní KII a VIS“, bod C.10.02 „Definovat soubor možných krizových situací a vytvářet krizové scénáře pro spolupráci, komunikaci a nasazení protiopatření v období krizových stavů“ a C.10.03 „Provádět národní cvičení v oblasti komunikace, koordinace a spolupráce při zajišťování kybernetické obrany“.	1
Celkový součet	**13**