Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020

K úspěšnému naplnění a dosažení hlavních cílů *Národní strategie kybernetické bezpečnosti pro období let 2015 až 2020* je zapotřebí dle stanoveného časového rámce realizovat či úspěšně naplňovat úkoly uvedené zde v *Akčním plánu k Národní strategii kybernetické bezpečnosti pro období let 2015 až 2020*.

U stanovených úkolů je vyžadována aktivní součinnost a spolupráce povinných subjektů ve smyslu zákona č. 181/2014 Sb., o kybernetické bezpečnosti, a dalších subjektů veřejné správy ČR v koordinaci a dle potřeb uvedeného odpovědného subjektu.

V tomto dokumentu jsou používány zkratky, jejichž vysvětlení je uvedeno na konci v sekci *Seznam použitých zkratek*.

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
A. Zajištění efektivity a posilování všech struktur, procesů a spolupráce při zajišťování kybernetické bezpečnosti				
Vytvořit efektivní model spolupráce na národní úrovni mezi jednotlivými subjekty kybernetické bezpečnosti – pracoviště typu CERT a CSIRT, subjekty KII apod. – a posilovat jejich stávající struktury a procesy.	**A.1.01**	Vytvořit v koordinaci s ostatními subjekty schéma a podrobný model spolupráce v rámci zajišťování kybernetické bezpečnosti.	NBÚ/NCKB *ve spolupráci s:* MV MZV MO MPO Zpravodajské služby	Q3 2015
	A.1.02	Provést analýzu agend v rámci problematiky kybernetické bezpečnosti a na jejím základě definovat národní zájmy a priority v této oblasti.	NBÚ/NCKB *ve spolupráci s:* MO MZV MPO Zpravodajské služby	Q4 2015
	A.1.03	Provádět technická i netechnická národní cvičení kybernetické bezpečnosti.	NBÚ/NCKB *ve spolupráci s:* MO MV Zpravodajské služby	průběžně

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
Vytvořit národní, koordinovaný postup pro zvládání incidentů, který nastaví formát spolupráce, bude obsahovat komunikační matici, protokol postupu a definovat jednotlivé role aktérů.	**A.2.01**	Vytvořit jednotnou metodologii pro zvládání kybernetických bezpečnostních incidentů na základě ZKB a souvisejících právních předpisů.	NBÚ/NCKB	Q1 2016
	A.2.02	Vytvořit komunikační matici mezi vrcholovými aktéry kybernetické bezpečnosti (národní aktéři, KII, VIS).	NBÚ/NCKB	Q2 2015
	A.2.03	Poskytnout popis bezpečné komunikace s datovým (komunikačním) rozhraním, pomocí kterého bude NBÚ automatizovaně přijímat XML zprávy s hlášením kybernetických bezpečnostních incidentů. Součástí bude i popis XML schématu, které odpovídá obsahu formuláře pro hlášení kybernetických bezpečnostních incidentů uvedeného ve vyhlášce č. 316/2014 Sb., doplněného o další nepovinná pole.	NBÚ/NCKB	Q2 2015
	A.2.04	Vytvořit protokol osvědčených postupů v oblasti zajišťování kybernetické bezpečnosti.	NBÚ/NCKB	Q2 2016
Vytvořit metodologii pro hodnocení rizik v ČR na úrovni státu.	**A.3.01**	Zvolit metodologii hodnocení rizik a hrozeb pro oblast kybernetické bezpečnosti na národní úrovni.	NBÚ/NCKB	Q1 2018
	A.3.02	Provádět hodnocení hrozeb a rizik pro oblast kybernetické bezpečnosti na národní úrovni.	NBÚ/NCKB	od Q2 2018 průběžně

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
Udržovat jednotný postoj ČR směrem do zahraničí, který bude koordinován s ostatními resorty zainteresovanými v oblasti kybernetické bezpečnosti.	**A.4.01**	Vytvořit efektivní model pro sdílení informací o zahraničních aktivitách mezi NBÚ a ostatními relevantními subjekty.	NBÚ/NCKB *ve spolupráci s:* MZV MO MPO MV ÚZSI	Q2 2016
	A.4.02	Koordinovat a harmonizovat s ostatními resorty pozice v EU, NATO a dalších mezinárodních organizacích.	NBÚ/NCKB *ve spolupráci s:* MZV MO MPO MV	od Q3 2015 průběžně
Zohledňovat odpovídajícím způsobem neustále se vyvíjející problematiku kybernetických hrozeb v rámci tvorby a aktualizací významných bezpečnostně-strategických materiálů ČR (Bezpečnostní strategie České republiky a další).	**A.5.01**	Implementovat Bezpečnostní strategii České republiky s ohledem na zvyšující se kybernetické hrozby a v případě změny bezpečnostního prostředí navrhnout její revizi.	NBÚ/NCKB MV MZV MO ÚV ČR Zpravodajské služby	průběžně

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
B. Aktivní mezinárodní spolupráce				
V rámci svého členství v EU, NATO, OSN, OBSE, ITU a dalších mezinárodních organizacích se bude ČR aktivně podílet na mezinárodní diskuzi v aktivitách v rámci fór, programů, iniciativ apod.	**B.1.01**	Spolupracovat s EU v implementaci Strategie kybernetické bezpečnosti EU.	NBÚ/NCKB MPO MZV MV	průběžně
	B.1.02	Aktivně spolupracovat s EU, Evropskou komisí a jejími agenturami k zajištění větší koherence v kybernetických tématech v rámci EU.	NBÚ/NCKB MPO MZV MV MO	průběžně
	B.1.03	Spolupracovat a aktivně se podílet na práci ENISA v oblasti informační a síťové bezpečnosti.	NBÚ/NCKB	průběžně
	B.1.04	Aktivně se podílet v OBSE na vytváření a následné implementaci kybernetických opatření pro zvyšování důvěry mezi státy v kyberprostoru a případně dalších iniciativ v souladu s vizemi a principy NSKB ČR.	NBÚ/NCKB *ve spolupráci s:* MZV	průběžně
	B.1.05	Spolupracovat se spojenci při implementaci politiky NATO v rámci kybernetické obrany.	NBÚ/NCKB MO VZ	průběžně
	B.1.06	Podporovat spolupráci s NATO v oblasti kybernetické obrany, zejména s ohledem na reakci na kybernetické bezpečnostní incidenty a výměnu technických informací o hrozbách a zranitelnostech.	NBÚ/NCKB MO MZV VZ	průběžně

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
	B.1.07	Podporovat spolupráci s ITU ve věci tvorby a zavádění technických standardů v kybernetické bezpečnosti.	NBÚ/NCKB MPO ČTÚ	průběžně
	B.1.08	Rozvíjet dialog skrze „cyber diplomacy“ mezi členskými zeměmi OSN týkající se norem vztahujících se k používání ICT v jednotlivých zemích s cílem snížit společné nebezpečí, chránit důležitou národní a mezinárodní infrastrukturu a budovat důvěru a stabilitu mezi zeměmi.	MZV *ve spolupráci s:* NBÚ/NCKB	průběžně
	B.1.09	Aktivně participovat národní expertizou a prostředky v CCDCOE a podílet se průběžně na výzkumných aktivitách centra.	NBÚ/NCKB MO	průběžně
Ve středoevropském prostoru působit jako propagátor kybernetické bezpečnosti a dialogu mezi státy regionu.	**B.2.01**	Aktivně se podílet a podporovat spolupráci jak v rámci V4, tak ve Středoevropské platformě kybernetické bezpečnosti (CECSP).	NBÚ/NCKB *ve spolupráci s:* MZV MO	průběžně
	B.2.02	Aktivně se podílet a podporovat spolupráci s národními bezpečnostními týmy ve středoevropském a východoevropském regionu.	NBÚ/NCKB MO	průběžně
Navazovat a prohlubovat bilaterální spolupráci s dalšími státy.	**B.3.01**	Pokračovat a prohlubovat bilaterální spolupráci s vybranými státy v rámci kybernetické bezpečnosti.	NBÚ/NCKB *ve spolupráci s:* MZV MO	průběžně
Účastnit se a organizovat mezinárodní cvičení.	**B.4.01**	Pravidelně se účastnit a aktivně se podílet na vytváření scénářů mezinárodních cvičení v oblasti kybernetické bezpečnosti.	NBÚ/NCKB MO MV	průběžně

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
Účastnit se a organizovat mezinárodní školení.	**B.5.01**	Účastnit se a organizovat mezinárodní školení, kurzy a semináře v oblasti kybernetické bezpečnosti.	NBÚ/NCKB *ve spolupráci s:* MZV MO MV Zpravodajské služby	průběžně
Podílet se na vytváření efektivního modelu spolupráce a budování důvěry mezi pracovišti typu CERT a CSIRT na mezinárodní úrovni, mezinárodními organizacemi a akademickými centry.	**B.6.01**	Podporovat vytváření mezinárodních komunikačních a informačních kanálů mezi CERT/CSIRT pracovišti, mezinárodními organizacemi a akademickými centry.	NBÚ/NCKB MO	průběžně
	B.6.02	Aktivně se zapojit do výstavby a užívání NATO projektů pro řízení reakcí na kybernetické bezpečnostní incidenty a výměnu technických informací o škodlivých kódech mezi státy NATO.	NBÚ/NCKB MO	od Q3 2015 průběžně
Podílet se na vytváření mezinárodního konsenzu v rámci oficiálních i neoficiálních kanálů ohledně právních norem a chování v kyberprostoru, zajištění otevřenosti internetu, lidských práv a svobod.	**B.7.01**	Zapojit se do mezinárodní diskuze ohledně tvorby a způsobů implementace mezinárodněprávních norem v kyberprostoru, vč. lidských práv.	NBÚ/NCKB *ve spolupráci s:* MZV	Q3 2015
	B.7.02	Zapojit se do mezinárodní diskuze ohledně správy a řízení internetu.	NBÚ/NCKB *ve spolupráci s:* MZV MPO MV	Q2 2015

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
C. Ochrana národní KII a VIS				
Pokračovat v průběžné analýze a kontinuálním sledování zabezpečení systémů KII a VIS v ČR pomocí jasně definovaného protokolu.	**C.1.01**	Určovat průběžně subjekty KII a identifikovat VIS, jichž se dotýká ZKB a související právní předpisy.	NBÚ/NCKB *Ve spolupráci s:* MV	průběžně
	C.1.02	Konzultovat, komunikovat a poskytovat metodickou podporu subjektům KII a VIS.	NBÚ/NCKB	průběžně
	C.1.03	Podporovat a průběžně kontrolovat implementaci zákonných povinností u subjektů KII a VIS.	NBÚ/NCKB	průběžně
	C.1.04	Spolupracovat s mezinárodními partnery při hodnocení určování KII, zejména v oblasti přeshraničních závislostí.	NBÚ/NCKB	průběžně
Podporovat vznik dalších pracovišť typu CERT a CSIRT v ČR.	**C.2.01**	Informovat o výhodách a aktivně podporovat u soukromých subjektů (především spadajících pod KII) vznik CERT/CSIRT týmů k zajištění lepší spolupráce při řešení kybernetických bezpečnostních incidentů.	NBÚ/NCKB	průběžně
	C.2.02	Podporovat vznik CERT/CSIRT týmů v rámci resortů, dalších institucí státní správy a v rámci různých průmyslových odvětví.	NBÚ/NCKB	průběžně
	C.2.03	Vybudovat resortní CERT/CSIRT pracoviště MV k ochraně základních registrů a nejdůležitějších systémů pro fungování e-Governmentu.	MV *ve spolupráci s:* NBÚ/NCKB	Q1 2016

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
Průběžně navyšovat odolnost, integritu a důvěryhodnost systémů a sítí KII a VIS.	**C.3.01**	Průběžně navyšovat kapacity NCKB, potažmo GovCERT.CZ a reflektovat personální a znalostní nároky vyplývající z vývoje stavu kybernetické bezpečnosti ve státě.	NBÚ/NCKB	průběžně
	C.3.02	Vytvořit doporučující základní rámec pro kybernetickou bezpečnost i mimo subjekty KII a VIS, tj. soubor standardů a osvědčených postupů, které pomohou organizacím zvládat kybernetická bezpečnostní rizika.	NBÚ/NCKB	Q3 2015
	C.3.03	Udržovat aktuální evidenci kybernetických bezpečnostních incidentů, vyhodnocovat je a navrhovat opatření.	NBÚ/NCKB	průběžně
	C.3.04	Určit minimální požadavky pro logy, které musí být zajištěny pro spolehlivou ex-post analýzu kybernetických bezpečnostních incidentů.	NBÚ/NCKB	Q4 2015
	C.3.05	Vytvořit a zavést honeypot systém k detekci kybernetických hrozeb.	NBÚ/NCKB	Q3 2016
	C.3.06	Mapovat vztahy mezi sítěmi veřejné správy a jejich ISP k zajištění efektivnější součinnosti v případě kybernetických bezpečnostních incidentů.	NBÚ/NCKB	od Q4 2015 průběžně

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
	C.3.07	Zajišťovat a metodicky řídit nasazování detekčních systémů pro monitorování provozu sítí a kybernetických bezpečnostních událostí v rámci státní správy.	NBÚ/NCKB	Q1 2017
	C.3.08	Vytvořit laboratoř pro detekci a testování dopadů malware na informační systémy.	NBÚ/NCKB	Q2 2016
	C.3.09	Vytvořit a rozvíjet scénáře a programy simulace kybernetických bezpečnostních incidentů využitelné pro účely národních cvičení.	NBÚ/NCKB *ve spolupráci s:* MO MV Zpravodajské služby	od Q3 2015 průběžně
	C.3.10	Vytvořit a používat kapacity a schopnosti pro provádění kybernetických bezpečnostních testů.	NBÚ/NCKB	od Q3 2015 průběžně
	C.3.11	Vytvořit kapacity a zlepšovat schopnosti forenzní analýzy a dalších podpůrných služeb v rámci kybernetické bezpečnosti pro potřeby ČR.	NBÚ/NCKB	od Q3 2015 průběžně
	C.3.12	Podporovat projekt Fénix a zapojení významných sítí veřejné správy za účelem zachování funkcionalit a služeb během masivních kybernetických útoků.	NBÚ/NCKB *ve spolupráci s:* MV	průběžně

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
Kontinuálně provádět analýzu a monitoring hrozeb a rizik v ČR.	**C.4.01**	Provádět sběr a analýzu informací o hrozbách a rizicích, a tím zajišťovat aktuální přehled o situaci v kybernetické bezpečnosti jak v ČR, tak i ve světě.	NBÚ/NCKB *ve spolupráci s:* Zpravodajské služby	průběžně
	C.4.02	Detekovat anomálie v síťovém provozu a identifikovat potenciální kybernetické hrozby.	NBÚ/NCKB	Q1 2016
	C.4.03	Rozvíjet schopnosti aktivně získávat informace v kyberprostoru o možných hrozbách a rizicích pro kybernetickou bezpečnost ČR.	Zpravodajské služby	průběžně
	C.4.04	Analyzovat obsah informací o hrozbách a rizicích pro důležité zájmy ČR získaných v kybernetickém prostoru včetně jejich manipulativního působení na veřejnost a vytvořit proces vzájemného efektivního informování o relevantních hrozbách a rizicích mezi příslušnými subjekty.	Zpravodajské služby *ve spolupráci s:* NBÚ/NCKB	průběžně
	C.4.05	Podporovat koordinaci při preventivním působení v oblasti kybernetické bezpečnosti a získávání informací k plánování kybernetických útoků s cílem předcházení jejich provedení.	BIS ÚZSI	průběžně
	C.4.06	Modernizovat a personálně posílit jednotlivé specializované útvary zpravodajských služeb.	BIS ÚZSI	od Q1 2016 průběžně

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
	C.4.07	Nastavit a rozvíjet spolupráci mezi zpravodajskými službami ČR i zainteresovanými věcně příslušnými národními či mezinárodními subjekty.	NBÚ/NCKB Zpravodajské služby	průběžně
Efektivně sdílet informace mezi státem a subjekty KII a VIS.	**C.5.01**	Zveřejňovat varování o kybernetických bezpečnostních hrozbách a incidentech s doporučením ke zvládání rizik.	NBÚ/NCKB	průběžně
	C.5.02	Vytvořit na základě dokončení mapování zabezpečovacích prvků u KII a VIS automatizovanou platformu na sdílení informací o kybernetických bezpečnostních hrozbách a incidentech vybraným ohroženým subjektům.	NBÚ/NCKB	Q4 2015
	C.5.03	Rozšířit možnosti hlášení kybernetických incidentů o webový formulář a komunikaci mezi systémy.	NBÚ/NCKB	Q1 2015
	C.5.04	Vytvořit na národní úrovni zabezpečenou platformu pro komunikaci při řešení rozsáhlejších kybernetických bezpečnostních incidentů.	NBÚ/NCKB	Q4 2015

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
Navyšovat technologické kapacity a schopnosti NCKB, potažmo GovCERT.CZ a v rovině personální neustále vzdělávat a školit zaměstnance tohoto pracoviště.	**C.6.01**	Průběžně vzdělávat a školit pracovníky NCKB v oblasti kybernetické bezpečnosti.	NBÚ/NCKB	průběžně
	C.6.02	Prostřednictvím zahraničních kurzů udržovat aktuální povědomí o trendech v kybernetické bezpečnosti a hrozbách, kterým ČR jako aktivní člen EU a NATO čelí.	NBÚ/NCKB	průběžně
	C.6.03	Navyšovat schopnosti GovCERT.CZ identifikovat povahu kybernetických bezpečnostních incidentů.	NBÚ/NCKB	od Q2 2016 průběžně
	C.6.04	Vybudovat a rozšiřovat detekční systém včasného varování GovCERT.CZ.	NBÚ/NCKB	Q3 2017
	C.6.05	Zavést v GovCERT.CZ nepřetržitý provoz pohotovostní služby k monitorování a řešení kybernetických bezpečnostních incidentů.	NBÚ/NCKB	Q1 2016
Důkladně a důvěryhodně zabezpečit prostředí pro skladování a práci s daty subjektů KII a VIS, které zřídí a bude spravovat stát.	**C.7.01**	Vytvořit a vládě předložit Národní strategii cloud computingu.	MV *ve spolupráci s:* MF NBÚ/NCKB	Q4 2015
	C.7.02	Vypracovat a vládě předložit projekt státního cloudu včetně datových uložišť a další potřebné podklady (finanční, bezpečnostní, organizační a technické nároky).	MV *ve spolupráci s:* MF NBÚ/NCKB	Q1 2016
	C.7.03	Zmapovat současný stav a případně vypracovat návrh legislativních změn s ohledem na vytvoření státního cloudu včetně datových uložišť.	MV *ve spolupráci s:* NBÚ/NCKB	Q1 2018

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
Pravidelně provádět kontrolu, odhalování chyb a zranitelností v informačních systémech a sítích využívaných státem, založené na principu penetračních testů v KII a VIS.	**C.8.01**	Pomocí předem ohlášených pravidelných penetračních testů provádět u subjektů KII a VIS odhalování chyb a zranitelnosti v jejich informačních systémech a sítích.	NBÚ/NCKB	Q1 2017
Průběžně navyšovat technologické a organizační předpoklady k aktivnímu odvracení (potlačení) kybernetických útoků.	**C.9.01**	V rámci Vojenského zpravodajství vytvořit Národní centrum kybernetických sil (NCKS), které bude schopné provádět široké spektrum operací v kyberprostoru a aktivity nutné pro zajištění kybernetické obrany ČR. NCKS bude schopné provádět vojenské operace v kyberprostoru, a to jak na podporu zahraničních operací AČR v rámci NATO nebo EU, tak i v případě hybridního konfliktu za účelem obrany ČR.	VZ	od Q1 2016 průběžně
	C.9.02	Připravit projekt financování a budování NCKS.	VZ	Q4 2015
	C.9.03	Zajištění vhodných prostor a nábor personálu pro NCKS.	VZ	od Q4 2015 průběžně
	C.9.04	Vybudování kompletní technické infrastruktury pro NCKS.	VZ	od Q1 2016 průběžně
	C.9.05	Připravit návrh nutných legislativních změn pro potřeby plné funkčnosti NCKS.	VZ *ve spolupráci s:* NBÚ/NCKB BIS ÚZSI	Q3 2015

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
Zvyšovat národní možnosti, schopnosti a kapacity v oblasti aktivní obrany a protiopatření proti kybernetickým útokům.	**C.10.01**	Plně zajišťovat kybernetickou obranu ČR skrze kooperaci NCKS, NCKB, národního CERT a ostatních pracovišť typu CERT/CSIRT.	VZ	Q1 2020
	C.10.02	Definovat soubor možných krizových situací a vytvářet krizové scénáře pro spolupráci, komunikaci a nasazení protiopatření v období krizových stavů.	NBÚ/NCKB *ve spolupráci s:* MO VZ	od Q3 2015 průběžně
	C.10.03	Provádět národní cvičení v oblasti komunikace, koordinace a spolupráce při zajišťování kybernetické obrany.	VZ *ve spolupráci s:* NBÚ/NCKB	od Q1 2017 průběžně
Vzdělávat specializované odborníky, kteří se zaměří na problematiku a možnosti aktivních protiopatření při zajišťování kybernetické bezpečnosti a obrany a na obecně ofenzivní pojetí kybernetické bezpečnosti.	**C.11.01**	Reflektovat v NCKB personální a znalostní nároky vyplývající z vývoje stavu kybernetické bezpečnosti ve světě a sdílet tyto své schopnosti a dovednosti s relevantními subjekty.	NBÚ/NCKB	průběžně
	C.11.02	Reflektovat v NCKS personální a znalostní nároky vyplývající z vývoje stavu kybernetické obrany ve světě.	VZ	průběžně

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
Zpracovat postup pro přechod mezi vyhlášeným stavem kybernetického nebezpečí dle zákona o kybernetické bezpečnosti a stavy dle ústavního zákona č. 110/1998 Sb., o bezpečnosti ČR.	**C.12.01**	Zpracovat postup pro přechod mezi vyhlášeným stavem kybernetického nebezpečí dle zákona o kybernetické bezpečnosti a stavy dle ústavního zákona č. 110/1998 Sb., o bezpečnosti ČR.	NBÚ/NCKB *ve spolupráci s:* MV MZV MO VZ ÚV ČR	Q1 2016
	C.12.02	Vytvořit pracovní skupinu z odborníků na mezinárodní právo z řad MO, MZV, MV, zpravodajských služeb a NBÚ/NCKB ve věci opatření kybernetické bezpečnosti a kybernetické obrany v mezinárodním měřítku.	NBÚ/NCKB *ve spolupráci s:* MV MZV MO Zpravodajské služby	Q3 2015

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
D. Spolupráce se soukromým sektorem				
Pokračovat v navazování spolupráce se soukromým sektorem a navyšovat povědomí o práci a aktivitách NBÚ v oblasti kybernetické bezpečnosti.	**D.1.01**	Navazovat kontakty a spolupráci se soukromým sektorem, a navyšovat tak povědomí o práci a možnostech spolupráce s NCKB prostřednictvím pravidelných jednání a vzájemného sdílení informací.	NBÚ/NCKB	průběžně
	D.1.02	Spolu s poskytovateli služeb elektronických komunikací a s poskytovateli služeb informační společnosti pracovat na shodném přístupu, jak lépe internetovým uživatelům v ČR pomoci rozpoznat a chránit se před škodlivými aktivitami v jejich systémech.	NBÚ/NCKB	průběžně
Vytvořit v kooperaci se soukromými subjekty jednotné bezpečnostní normy, standardizovat spolupráci a stanovit povinnou úroveň zabezpečení pro subjekty KII.	**D.2.01**	Spolupracovat se soukromoprávními subjekty KII při vytváření požadavků na bezpečnostní normy a povinné úrovně zabezpečení pro subjekty KII.	NBÚ/NCKB	průběžně
	D.2.02	Podporovat rozvoj norem v oblasti kybernetické bezpečnosti prostřednictvím národních a mezinárodní standardizačních a certifikačních orgánů a institucí a podporovat jejich přijetí u soukromých subjektů.	NBÚ/NCKB	průběžně

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
Zajistit v kooperaci se soukromým sektorem kyberprostor poskytující spolehlivé prostředí pro sdílení informací, výzkum a vývoj a zajistit bezpečnou informační infrastrukturu stimulující podnikání soukromých subjektů v zájmu podpory konkurenceschopnosti všech podnikajících soukromých subjektů v ČR a chránící jejich investice.	**D.3.01**	Propagovat vysokou úroveň kybernetické bezpečnosti ve veřejných službách, a tím maximalizovat využívání systémů eGovernmentu ze strany soukromých organizací i široké veřejnosti.	MPO MV	průběžně
	D.3.02	Koordinovat přechod z protokolu IPv4 na IPv6 a informovat o bezpečnostních rizicích s tímto přechodem spjatých.	MPO *ve spolupráci s:* MV	průběžně
	D.3.03	Podporovat rozšiřování DNSSEC pro zabezpečení webových prezentací a pravidelně monitorovat stav implementace DNSSEC jak ve veřejné správě, tak v národní doméně.cz.	MPO	průběžně
Vzdělávat a provádět osvětu soukromého sektoru v oblasti kybernetické bezpečnosti. Soukromým subjektů tak poskytnout potřebné vedení, jak se správně chovat nejen při mimořádných situacích, respektive při kybernetických incidentech, ale i při každodenní činnosti.	**D.4.01**	Poskytovat poradenství a organizovat vzdělávací a osvětové aktivity pro subjekty soukromé sféry.	NBÚ/NCKB	průběžně
	D.4.02	Podporovat malé a středně velké podniky prostřednictvím informační kampaně ohledně kybernetické bezpečnosti úzce zaměřené na potřeby a jejich možnosti.	NBÚ/NCKB MPO	průběžně
Navyšovat důvěru mezi soukromým sektorem a státem, mimo jiné vytvořením platformy/systému na národní úrovni pro sdílení informací o hrozbách, incidentech a aktuálním ohrožení.	**D.5.01**	Vytvořit mezi NCKB a subjekty KII a VIS platformu na sdílení informací o kybernetických hrozbách a zranitelnostech.	NBÚ/NCKB	Q1 2016

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
E. Výzkum a vývoj / Spotřebitelská důvěra				
Podílet se na národních i evropských výzkumných projektech a aktivitách v oblasti kybernetické bezpečnosti.	**E.1.01**	Zmapovat současný stav VaV zabývajícího se kybernetickou bezpečností a technologiemi používanými v ČR.	NBÚ/NCKB *ve spolupráci s:* MV MO	Q1 2018
	E.1.02	Ve spolupráci s ostatními organizačními složkami státu vypracovat národní koncepci VaV v oblasti kybernetické bezpečnosti.	NBÚ/NCKB *ve spolupráci s:* MV MO Policie ČR TAČR Zpravodajské služby	Q3 2018
	E.1.03	Vypracovat a plnit plán výzkumných aktivit NBÚ v oblasti kybernetické bezpečnosti s ohledem na současné a budoucí potřeby státu.	NBÚ/NCKB *ve spolupráci s:* MO Zpravodajské služby	Q3 2017

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
Určit NBÚ jako hlavní kontaktní centrum v oblasti výzkumu v kybernetické bezpečnosti. NBÚ bude přispívat ke koordinaci výzkumných aktivit v této oblasti s cílem zabránit zdvojování výzkumných aktivit. Výzkum v oblasti kybernetické bezpečnosti se tak zaměří na opravdu podstatné problémy a převod výzkumných výsledků do praxe.	**E.2.01**	Vytvořit databázi výzkumných projektů v rámci kybernetické bezpečnosti a podávat z ní informace dalším subjektům.	NBÚ/NCKB	Q1 2019
	E.2.02	Zřídit pracovní skupinu zastoupenou všemi organizačními složkami státu zabývajícími se VaV v oblasti kybernetické bezpečnosti, tj. zejména NBÚ/NCKB, MV, MO, TAČR a zpravodajské služby.	NBÚ/NCKB *ve spolupráci s:* MV MO TAČR Zpravodajské služby	Q3 2017
Spolupracovat se soukromým a akademickým sektorem na vývoji a implementaci technologií využívaných státem k zajištění jejich maximálního zabezpečení a transparentnosti. Testovat a hodnotit míru zabezpečení používaných technologií.	**E.3.01**	Iniciovat a podílet se na realizaci výzkumných projektů s partnery ze soukromé sféry.	NBÚ/NCKB	průběžně
Spolupracovat s akademickou a soukromou sférou na výzkumných projektech (včetně primárního i experimentálního výzkumu) a aktivitách v technologické i společenskovědní oblasti, a to především na národní, evropské i mezinárodní transatlantické úrovni.	**E.4.01**	Spolupracovat s akademickou a soukromou sférou na výzkumných projektech, poskytovat jim potřebné informace a strategické vedení. Zapojit ČR a její akademickou i soukromou sféru do výzkumných programů (zahrnujících základní i aplikovaný výzkum a vývoj) na evropské i mezinárodní a transatlantické úrovni.	NBÚ/NCKB MŠMT	průběžně
	E.4.02	Podporovat a podílet se na publikační činnosti akademické sféry v oblasti kybernetické bezpečnosti.	NBÚ/NCKB	průběžně
Hlavní cíle	**Kód**	**Úkoly**	**Odpovědný subjekt**	**Časový rámec**

F. Podpora vzdělávání, osvěta a rozvoj informační společnosti

Navyšovat povědomí a gramotnost v otázkách kybernetické bezpečnosti jak u žáků a studentů základních a středních škol, tak i u široké veřejnosti, respektive koncových uživatelů, pomocí podpory iniciativ a osvětových kampaní, pořádáním konferencí pro veřejnost apod.	**F.1.01**	Podporovat iniciativy a osvětové kampaně, pořádat konference a workshopy pro veřejnost, respektive koncové uživatele.	NBÚ/NCKB *ve spolupráci s:* MPSV	průběžně
	F.1.02	Provozovat a kontinuálně aktualizovat portál GovCERT.CZ jako informační platformu pro veřejnost ohledně aktuálních bezpečnostních hrozeb, rizik, zranitelností a dalších aktivit NBÚ.	NBÚ/NCKB	průběžně
	F.1.03	Vytvořit e-learningovou platformu pro vzdělávání širší a odborné veřejnosti.	NBÚ/NCKB *ve spolupráci s:* MPSV	Q1 2016
Modernizovat stávající vzdělávací programy na základní a středoškolské úrovni a podporovat na vysokoškolské úrovni nové studijní programy, které budou přímo vzdělávat experty na kybernetickou bezpečnost.	**F.2.01**	Modernizovat rámcové vzdělávací programy na základní a středoškolské úrovni.	NBÚ/NCKB MŠMT	Q1 2017
	F.2.02	Připravit metodické pokyny a materiály usnadňující školám zapracování problematiky kybernetické bezpečnosti do školních vzdělávacích programů podle nových rámcových vzdělávacích programů.	NBÚ/NCKB MŠMT	Q1 2017
	F.2.03	Připravit dostatek metodických materiálů pro učitele, zajistit vzdělávání učitelů v této oblasti a připravit dostatek výchozích učebních materiálů pro žáky.	NBÚ/NCKB MŠMT	Q1 2017
	F.2.04	Vytvořit přehled vysokoškolských studijních programů v ČR i zahraničí zabývajících se kybernetickou bezpečnostní, průběžně jej aktualizovat a tento přehled v rámci propagace zveřejňovat.	NBÚ/NCKB	Q4 2015

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
	F.2.05	Zvyšovat povědomí ohledně zodpovědného, bezpečného používání internetu, ICT a nových médií.	NBÚ/NCKB *ve spolupráci s:* MPSV	průběžně
	F.2.06	Podporovat u studentů rozvoj talentu v oblasti kybernetické bezpečnosti ve spolupráci s vysokými školami.	NBÚ/NCKB	průběžně
	F.2.07	Zprostředkovávat vysokoškolským studentům možnost stáže v oblasti kybernetické bezpečnosti v ČR i zahraničí.	NBÚ/NCKB MO	průběžně
	F.2.08	Spolupracovat na vytváření nových vysokoškolských studijních oborů v oblasti kybernetické bezpečnosti a kybernetické obrany a spolupracovat s univerzitami a vysokými školami při zavádění těchto nových oborů, tvorbě učebních plánů apod.	NBÚ/NCKB MO	průběžně

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
Vzdělávat a školit zaměstnance veřejné správy působící nejen v oblasti kybernetické bezpečnosti a informační kriminality.	**F.3.01**	Školit stávající zaměstnance veřejné správy v oblasti kybernetické bezpečnosti.	NBÚ/NCKB MPSV MV	Od Q4 2015 průběžně
	F.3.02	Školit manažery kybernetické bezpečnosti ve veřejné správě ve věci rozpoznávání, (např. detekování anomálií), hlášení kybernetických bezpečnostních incidentů a další spolupráce s NCKB.	NBÚ/NCKB MPSV	průběžně
	F.3.03	Institucionalizovat další vzdělávání prostřednictvím získávání osvědčení za absolvování vzdělávacích programů.	NBÚ/NCKB MPSV MV	průběžně
	F.3.04	Pomocí moderních výukových metod zvyšovat úroveň vzdělanosti v oblasti kybernetické bezpečnosti.	NBÚ/NCKB MPSV	průběžně

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
G. Podpora rozvoje schopností PČR vyšetřovat a postihovat informační kriminalitu				
Posílit personálně jednotlivá policejní pracoviště informační kriminality.	**G.1.01**	Personálně posílit pracoviště informační kriminality Policejního prezidia ČR o systemizovaná služební místa a systemizovaná pracovní místa, která budou sanovat stávající krizový stav a dále nyní naplní nezbytný lidský potenciál pro plnění vyžadovaných a stanovených činností.	Policie ČR MV	do 2018
	G.1.02	Personálně posílit o systemizovaná služební místa, ÚOOZ SKPV, ÚOKFK SKPV a NPC SKPV s ohledem na vyšetřování návazné trestné činnosti související s informační kriminalitou, včetně oblasti boje s terorismem zasahujícím i prostředí informačních technologií.	Policie ČR MV	do 2018
	G.1.03	Personálně posílit jednotlivá regionální výkonná pracoviště SKPV určených pro informační kriminalitu o systemizovaná služební místa a systemizovaná služební místa v jednotlivých krajích. Tímto se sleduje reakce na lokální situaci v rámci regionálních součástí SKPV dle modelu respektujícího rozdělení na technický, operativní a procesní aspekt zastoupení na příslušném pracovišti informační kriminality, zajištěním dostatečné sanace stávajícího stavu, pokrytí vedení odborně náročného trestního řízení a zajištění akceschopnosti.	Policie ČR MV	do 2018

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
	G.1.04	Personálně posílit infastrukturu regionálních znaleckých pracovišť PČR o systemizovaná služební místa. Kriminalistický ústav Praha v souvislosti s jeho republikovou působností posílit o systemizovaná služební místa, která budou sanovat stávající nesoulad poměru zajišťované činnosti a personálních kapacit.	Policie ČR MV	do 2018
	G.1.05	Personálně posílit ÚZČ SKPV v oblasti programování o systemizovaná služební místa, v oblasti technické správy systémů o systemizovaná služební místa, která budou zajišťovat přijímání, zpracování a vyřizování rostoucích požadavků a zejména objemu dat charakteru provozních a lokalizačních údajů sítě Internet.	Policie ČR MV	do 2018
	G.1.06	Personálně posílit o systemizovaná služební místa ÚSČ SKPV pro podporu speciálních činností v souvislosti s penetrací informačních technologií i do oblastí zajišťování úkonů souvisejících s vyšetřováním trestné činnosti	Policie ČR MV	do 2018
	G.1.07	Personálně posílit technologickou správu dat a informační podporu zabezpečovanou pracovišti informatiky a provozu informačních technologií.	Policie ČR MV	do 2018

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
Modernizovat technologické vybavení odborných policejních pracovišť.	**G.2.01**	Nastavit povinnou a vynutitelnou minimální technologickou vybavenost všech pracovišť OIK SKPV a zajistit stanovenou techniku a technologie.	Policie ČR MV	do 2018
	G.2.02	Nastavit povinnou a vynutitelnou minimální technologickou vybavenost všech znaleckých pracovišť tzv. počítačové analýzy a zajistit stanovenou techniku a technologie.	Policie ČR MV	do 2018
	G.2.03	Společně plánovat jednotlivé nákupy pro výkonná pracoviště OIK a znalecká pracoviště počítačové analýzy s garancí vázanosti plánovaných prostředků v plánovaných rozpočtech pro další údobí.	Policie ČR MV	do 2018
	G.2.04	Postupně realizovat vzájemnou blízkost dislokací výkonných a znaleckých pracovišť SKPV na jednotlivých úrovních v závislosti na vývoji stávajících dislokací.	Policie ČR MV	do 2018
Zakotvit vazby přímé a rychlé spolupráce se zainteresovanými národními subjekty a ostatními bezpečnostními složkami pro oblast informační kriminality.	**G.3.01**	Vytvořit smluvní či obdobné vazby umožňující a garantující přímou a časově nejrychlejší spolupráci na prováděcí úrovni s bezpečnostními složkami BIS, ÚZSI a VZ a s prvky kritické infrastruktury, NCKB, GovCERT.CZ a národním CERT.	Policie ČR MV *ve spolupráci s:* Vojenská policie	Q3 2016
Hlavní cíle	**Kód**	**Úkoly**	**Odpovědný subjekt**	**Časový rámec**

Podpořit spolupráci se zahraničními subjekty v oblasti výměny informací k informační kriminalitě a v oblasti vzdělávání.	**G.4.01**	Spolupracovat se zahraničními subjekty v oblasti výměny informací k informační kriminalitě a v oblasti vzdělávání.	Policie ČR MV *Ve spolupráci s:* Vojenská policie	průběžně
Odborně vzdělávat a školit policejní specialisty.	**G.5.01**	Rozšířit kurzy kvalifikační přípravy o základní znalosti a dovednosti spojené s kriminalitou páchanou v prostředí informačních technologií a zavést elektronický nebo obdobně plošně nasaditelný systém průběžného vzdělávání.	Policie ČR MV	průběžně, do Q2 2017
	G.5.02	Rozšířit specializační kurzy pro policisty SKPV o vyšší znalosti a dovednosti spojené s kriminalitou páchanou v prostředí informačních technologií.	Policie ČR MV	průběžně, do Q2 2017
	G.5.03	Připravit odborné kurzy policejních specialistů na kriminalitu páchanou v prostředí informačních technologií.	Policie ČR MV	průběžně, do Q2 2017
	G.5.04	Vytvořit podmínky pro průběžné vzdělávání expertů PČR v oblasti informační kriminality v komerčním a akademickém prostředí.	Policie ČR MV	průběžně, do Q2 2017

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
	G.5.05	Kapacitně posílit a rozšířit podmínky pro jazykové studium specialistů ve formě všeobecné jazykové přípravy, odborné jazykové přípravy a zdokonalovacích kurzů a souběžně zohlednit další nábory s preferencí jazykové vybavenosti.	Policie ČR MV	průběžně, do roku 2017
Vybudovat multidisciplinární akademické prostředí pro podporu rozvoje schopností PČR postihovat informační kriminalitu.	**G.6.01**	Vybudovat multidisciplinární formalizované akademické prostředí rozvoje schopnosti bezpečnostních složek a zejména PČR postihovat informační kriminalitu a řešit s tím spojené bezpečnostní, standardizační, normotvorné, výzkumné a další provázané potřeby.	Policie ČR MV	průběžně do roku 2018

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
H. Právní úprava pro kybernetickou bezpečnost (vytváření právního rámce) Účast na tvorbě a implementaci evropských a mezinárodních pravidel				
Na základě systematického přístupu, tj. vzhledem k existujícím právním předpisům, vytvářet v oblasti kybernetické bezpečnosti srozumitelné, efektivní a proporcionální právní předpisy.	**H.1.01**	Vytvářet v oblasti kybernetické bezpečnosti srozumitelné, efektivní a proporcionální zákonné a podzákonné právo.	NBÚ/NCKB *ve spolupráci s:* MZV	průběžně
	H.1.02	Analyzovat nezbytné zákonné regulace pro účinné zajištění kybernetické bezpečnosti v ČR.	NBÚ/NCKB *ve spolupráci s:* MZV	průběžně
Aktivně se účastnit tvorby a implementace evropských a mezinárodních pravidel.	**H.2.01**	Kontinuálně se podílet na vývoji a implementaci evropského a mezinárodního právního rámce a pravidel v oblasti kybernetické bezpečnosti.	NBÚ/NCKB MZV	průběžně
	H.2.02	Účastnit se diskuzí nad pojetím a významem konceptů kybernetické bezpečnosti a kybernetické obrany.	NBÚ/NCKB MZV MO MV Zpravodajské služby	průběžně

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
Provádět jak kontinuální analýzu efektivity účinné právní úpravy a jejího souladu s aktuálními poznatky z dotčených technických a společenskovědních oborů, tak i průběžné provádění změn a doplňování tak, aby právní úprava odpovídala aktuálním požadavkům bezpečné informační společnosti.	**H.3.01**	Na základě průběžné analýzy efektivity účinné právní úpravy a jejího souladu s aktuálními poznatky z dotčených technických a společenskovědních oborů provádět příslušné změny a doplňování.	NBÚ/NCKB	průběžně
	H.3.02	Nastavovat povinnou úroveň zabezpečení pro subjekty KII pomocí aktualizace zákonného a podzákonného práva.	NBÚ/NCKB	průběžně
	H.3.03	Provést revizi a vytvořit návrh legislativních změn vybraných paragrafů trestního zákoníku a zákona o elektronických komunikacích, které by zefektivnily vyšetřování a postihování informační kriminality a reflektovaly aktuální situaci v problematice informační kriminality.	MV Policie ČR ČTÚ *ve spolupráci s:* Zpravodajské služby	Q1 2016
Podporovat vzdělávání v problematice kybernetické bezpečnosti v rámci justičních orgánů (tj. státních zástupců nebo soudců).	**H.4.01**	Pomocí vzdělávání soudců a státních zástupců ohledně kybernetické problematiky zajistit ukládání a vymáhání přiměřených sankcí v trestněprávních sporech, které zahrnují kybernetickou problematiku.	NBÚ/NCKB MS MV Policie ČR	průběžně

SEZNAM POUŽITÝCH ZKRATEK

BIS – Bezpečnostní informační služba

CCDCOE – Cooperative Cyber Defence Centre of Excellence

CECSP – Central European Cyber Security Platform

CERT – Computer Emergency Response Team

CSIRT – Computer Security Incident Response Team

ČR – Česká republika

ČTÚ – Český telekomunikační úřad

DNSSEC – Domain Name System Security Extensions – sada specifikací umožňující zabezpečit informace poskytované DNS systémem v IP sítích

ENISA – European Union Agency for Network and Information Security – Evropská agentura pro bezpečnost sítí a informací

EU – Evropská unie

ICT – Informační a komunikační technologie

IPv4 – Internet Protocol version 4

IPv6 – Internet Protocol version 6

ISP – internet service provider – poskytovatel internetového připojení

ITU – Mezinárodní telekomunikační unie

KII – Kritická informační infrastruktura

MF – Ministerstvo financí

MO – Ministerstvo obrany

MPO – Ministerstvo průmyslu a obchodu

MS – Ministerstvo spravedlnosti

MŠMT – Ministerstvo školství, mládeže a tělovýchovy

MV – Ministerstvo vnitra

MZV – Ministerstvo zahraničních věcí

NATO – Severoatlantická aliance (North Atlantic Treaty Organization)

NBÚ/NCKB – Národní bezpečnostní úřad / Národní centrum kybernetické bezpečnosti

NCKS – Národní centrum kybernetických sil

NPC SKPV – Národní protidrogová centrála služby kriminální policie a vyšetřování

NSKB – Národní strategie kybernetické bezpečnosti

OBSE – Organizace pro bezpečnost a spolupráci v Evropě

OIK SKPV – Oddělení informační kriminality služby kriminální policie a vyšetřování

PČR – Policie ČR

TAČR – Technologická agentura ČR

ÚZSI – Úřad pro zahraniční styky a informace

ÚOKFK SKPV – Útvar odhalování korupce a finanční kriminality služby kriminální policie a vyšetřování

ÚOOZ SKPV – Útvar pro odhalování organizovaného zločinu služby kriminální policie a vyšetřování

ÚSČ SKPV – Útvar speciálních činností služby kriminální policie a vyšetřování

ÚZČ SKPV – Útvar zvláštních činností služby kriminální policie a vyšetřování

ÚV ČR – Úřad vlády ČR

V4 – Visegrádská skupina

VaV – Výzkum a vývoj

VIS – Významné informační systémy

VZ – Vojenské zpravodajství

XML – Extensible Markup Language – obecný značkovací jazyk

ZKB – Zpráva o kybernetické bezpečnosti

Zpravodajské služby – BIS, ÚZSI a VZ