Národní plán výzkumu a vývoje v oblasti kybernetické a informační bezpečnosti do roku 2020

OBSAH

Úvod

Dynamický rozvoj informačních a komunikačních technologií přináší nejen nová řešení technických a společenských problémů, ale také nové výzvy spjaté s bezpečností kybernetického prostoru ČR. Stát proto musí být schopen čelit kybernetickým hrozbám, jejichž počet a důmyslnost roste[1]. Například systémy využívající prvky strojového učení a umělé inteligence umožňují analyzovat velké množství dat, což vede k rostoucímu množství sofistikovaných spear-phishingových útoků. Postupující integrace fyzických zařízení do počítačově řízených systémů (Internet věcí – IoT) klade vyšší nároky na jejich zabezpečení, obdobně je tomu i v případě postupující digitalizace průmyslových sítí. Kybernetická bezpečnost je tak úzce spjata s výzkumem, vývojem a inovacemi (dále jen „VaVaI“), což se také odráží v:

- Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020 (dále jen „Národní strategie“)[2];
- Bezpečnostní strategii České republiky[3];
- Auditu národní bezpečnosti z roku 2016[4];
- Aktualizaci Národní politiky výzkumu, vývoje a inovací České republiky na léta 2016 – 2020 (aktualizace 2018)[5];
- Meziresortní koncepci podpory bezpečnostního výzkumu ČR 2017 – 2023 s výhledem do roku 2030[6].

Základní strategický rámec zajišťování kybernetické bezpečnosti v ČR definuje Národní strategie a navazující Akční plán, který byl schválen usnesením vlády č. 382 ze dne 25. května 2015. Toto usnesení ukládá Národnímu úřadu pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) vypracovat Národní koncepci výzkumu a vývoje v kybernetické bezpečnosti[7]. Avšak s ohledem na dynamiku vývoje řešené problematiky a zkušenosti bylo shledáno, že požadavky vědy a vývoje v oblasti kybernetické bezpečnosti lépe naplňuje jiný typ materiálu – Národní plán, který se dle Metodiky přípravy veřejných strategií, vypracované

[1] Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2018, dostupná zde: https://www.nukib.cz/download/publikace/zprava-o-stavu-kyberneticke-bezpecnosti-cr-2018-cz.pdf
[2] Dokument dostupný zde: https://www.govcert.cz/cs/informacni-servis/strategie-akcni-plan/
[3] Dokument dostupný zde: https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf
[4] Dokument dostupný zde: https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf
[5] Dokument dostupný zde: https://www.vyzkum.cz/FrontClanek.aspx?idsekce=866175
[6] Dokument dostupný zde: https://www.mvcr.cz/vyzkum/clanek/koncepce-meziresortni-koncepce-podpory-bezpecnostniho-vyzkumu-cr.aspx
[7] Dokumenty dostupné zde: https://www.govcert.cz/cs/informacni-servis/strategie-akcni-plan/

MMR z roku 2018[8], zaměřuje na řešení konkrétních cílů a identifikaci nástrojů k jejich dosažení. Součástí každé kapitoly jsou zároveň analytická východiska odpovídající definici koncepčního dokumentu.

Cílem předkládaného Národního plánu je **identifikovat prioritní výzkumná témata v oblasti kybernetické a informační bezpečnosti, která jsou klíčová pro rozvoj systému zabezpečení kyberprostoru ČR** a zároveň **stanovit další rozvojové cíle včetně konkrétních nástrojů, které přispějí ke koordinaci výzkumných aktivit, spolupráci se soukromým a akademickým sektorem na vývoji a implementaci technologií a k celkovému rozvoji výzkumného a inovačního prostředí v prioritních výzkumných tématech**. Národní plán vznikal v úzké spolupráci se subjekty veřejné, akademické a podnikatelské sféry s cílem zajistit co nejširší shodu nad obsahem dokumentu[9].

Platnost Národního plánu je stanovena do roku 2020. Vyhodnocení naplňování cílů Národního plánu bude součástí Hlášení o stavu naplňování Akčního plánu k Národní strategii kybernetické bezpečnosti ČR, které je přílohou Zprávy o stavu kybernetické bezpečnosti za uplynulé období. Vyhodnocení bude probíhat na základě plnění a hodnocení úkolů stanovených Akčním plánem. Informace o plnění jednotlivých opatření bude také předložena na jednání Platformy k výzkumu a vývoji v kybernetické a informační bezpečnosti (kapitola 3.2.).

1 Působnost NÚKIB v systému podpory VaVaI v kybernetické bezpečnosti

NÚKIB je ústředním správním orgánem pro kybernetickou bezpečnost ČR a zajišťuje:

- ochranu informačních a komunikačních systémů spadajících pod zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů,
- ochranu informačních a komunikačních systémů spadajících pod zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů,

[8] Dokument dostupný zde: https://www.mmr.cz/getmedia/08a14dd9-27e8-4a3c-a5cc-532936845297/Metodika-pripravy-verejnych-strategii-zkracena-verze_1.pdf.aspx?ext=.pdf.

[9] V průběhu přípravy Národního plánu NÚKIB oslovil celkem 16 partnerů s žádostí o jejich vstupy a proběhlo několik dvoustranných jednání se zástupci veřejné, akademické a soukromé sféry. Příkladem jsou MV, ÚV, MMR, MPO, MŠMT, dále pak s experty z ČVUT, VUT v Brně či Masarykovy univerzity. Národní plán byl rovněž diskutován v rámci pracovní skupiny, kde jsou zastoupeny organizační složky státu zabývající se výzkumem a vývojem v oblasti kybernetické bezpečnosti (BIS, ÚZSI, Policie ČR, apod.).

- kryptografickou ochranu a
- veřejně regulovanou službu satelitního systému Galileo.

NÚKIB není poskytovatelem účelové a institucionální podpory dle zákona č. 130/2002 Sb., o podpoře výzkumu a vývoje z veřejných prostředků a o změně některých souvisejících zákonů (zákon o podpoře výzkumu a vývoje), ve znění pozdějších předpisů. Zákon o kybernetické bezpečnosti a zákon o ochraně utajovaných informací mu však ukládají **zajišťovat výzkum a vývoj v oblasti kybernetické bezpečnosti, ve vybraných oblastech ochrany utajovaných informací a národních kryptografických prostředků.** V praxi tak NÚKIB působí nejen jako zadavatel veřejných zakázek pro potřeby NÚKIB, ale rovněž jako koncový uživatel výsledků VaVaI.

NÚKIB se dále bude podílet na vytváření informačního a analytického zázemí pro bezpečnostní komunitu a přispívat ke koordinaci výzkumných aktivit včetně identifikace výzkumných potřeb, problémů a priorit v kybernetické a informační bezpečnosti[10]. Rolí NÚKIB je také zajistit maximální zabezpečení a transparentnost technologií využívaných státem, včetně testování míry zabezpečení používaných technologií a jejich efektivnější využití v praxi. Činnost NÚKIB v oblasti VaVaI tak není v rozporu s působností organizačních složek státu poskytujících veřejnou podporu v oblasti VaVaI, ale naopak ji doplňuje a rozvíjí.

2 Prioritní výzkumná témata kybernetické a informační bezpečnosti

Omezené zdroje, které jsou pro podporu VaVaI v oblasti kybernetické a informační bezpečnosti k dispozici, je nutné soustředit do několika klíčových výzkumných oblastí. Proto byla ve spolupráci s experty NÚKIB a dalšími odborníky z akademické a podnikatelské sféry identifikována **prioritní výzkumná témata, jejichž stabilní podpora je klíčovým předpokladem pro plnění úkolů NÚKIB s ohledem na současné a budoucí potřeby státu**, a to v oblastech ochrany prvků kritické informační infrastruktury (dále jen „KII“), významných informačních systémů (dále jen „VIS“), systémů provozovatelů základní služby, komunikačních systémů kritické informační infrastruktury[11], systémů nakládajících s utajovanými informacemi a kryptografie[12].

[10] NÚKIB rovněž provádí aktivity zaměřené na vzdělávání v oblasti kybernetické bezpečnosti směrem ke státním institucím i veřejnosti. Informace o systému výzkumu a také informace zachycené z výzkumného pole jsou v závislosti na cílovém publiku zakomponovány i do vzdělávacích aktivit.
[11] Zákon č. 181/2014 Sb. o kybernetické bezpečnosti.
[12] Zákon č. 412/2005 Sb. o ochraně utajovaných informací a bezpečnostní způsobilosti.

Výchozí stav:

S technologickým rozvojem se mění metody útoků, jejich sofistikovanost a síla. Dle Zprávy o stavu kybernetické bezpečnosti ČR za rok 2018 čelí Česko významnému nárůstu počtu spear-phishingových útoků, které útočníci využívají k získání přístupu do cílové sítě. Dle Klasifikace řešených incidentů v roce 2018[13] tak vzrostl počet podvodných incidentů využívající metod phishingu a spear-phishingu na dvojnásobek oproti roku 2016[14].

Jednou z dalších výzev kybernetické bezpečnosti je schopnost čelit exponenciálnímu nárůstu síly DDoS (distributed denial of service) útoků, jejichž cílem je omezit dostupnost služeb. Příkladem mohou být DDoS útoky na volební proces v letech 2017 a 2018. V roce 2018 představovaly útoky za účelem narušení dostupnosti služeb celkem 33 % všech incidentů hlášených v GovCERT. Narůstající počet útoků související s pokročilým sociálním inženýrstvím klade vysoké nároky na schopnost státu chránit své sítě a další prvky KII a VIS. S narůstající digitalizací průmyslových sítí a SCADA systémů tak lze očekávat zvyšující se tlak na výzkum a vývoj ochranných nástrojů, které budou schopny lépe chránit komunikační a informační sítě. Příklady těchto nástrojů jsou automatizace penetračního testování či pokročilý monitoring síťového provozu včetně sběru dat pro forenzní analýzu.

V souvislosti s nárůstem počtu IoT zařízení, rozvojem technologií zvyšující konektivitu (5G sítě) a stále většího vytěžování cloudové infrastruktury roste potenciál využití (a zneužití) aplikací využívajících prvky umělé inteligence. Je proto zapotřebí soustředit úsilí do výzkumu a vývoje nástrojů pro analýzu velkých objemů dat a automatizace řešení kybernetických bezpečnostních událostí.

Výzkumná témata v oblasti kryptografické ochrany a vývoje kryptografických prostředků vychází z vnitřních potřeb NÚKIB na zajišťování kryptografické ochrany a dále z konzultací s experty v daných oblastech. Jedná se o témata zaměřená například na vývoj speciálních měřících metod a technologií při zajišťování ochrany před kompromitujícím elektromagnetickým vyzařováním či výzkum a vývoj kryptografických algoritmů odolných vůči prolomení, například v oblasti výzkumu postkvantové kryptografie.

[13] Zpráva o stavu kybernetické bezpečnosti ČR za rok 2018.
[14] Zpráva o stavu kybernetické bezpečnosti ČR za rok 2016.

2.1 Prioritní výzkumná témata v oblasti ochrany prvků KII, VIS a systémů provozovatelů základní služby:

- Pokročilé metody a automatizace penetračního testování,
- analýza síťové komunikace a vývoj unikátních detekčních technik v síťovém provozu s využitím pokročilého managementu bezpečnostních informací a threat intelligence,
- nové metody ochrany před DDoS útoky,
- bezpečnost průmyslových sítí a systémů SCADA/ICS v souvislosti s rozvojem IoT a připojením ke cloudu,
- rozvoj technologií a metod zvyšující ochranu před narušením soukromí a ztrátou identity,
- ochrana proti sofistikovaným formám spear-phishingu,
- výzkum a vývoj algoritmů umělé inteligence posilujících kybernetickou bezpečnost a odolnost strategických sítí a systémů státu,
- forenzní šetření – rozvoj nástrojů pro práci s elektronickými důkazními prostředky,
- vývoj metod postkvantové kryptografie schopné odolat kvantovým útokům,
- ochrana před sofistikovanými formami malware,
- podpora rozvoje systému certifikace a standardů kybernetické bezpečnosti,
- bezpečnostní politika, vývojové perspektivy legislativy kybernetické bezpečnosti, tvorba krizových scénářů a metodik v oblasti kybernetické bezpečnosti,
- vývoj nástrojů pro simulace a technická cvičení v kybernetické bezpečnosti,
- uplatnění distribuované decentralizované databáze (blockchain) v kybernetické bezpečnosti.

2.2 Prioritní výzkumná témata v oblasti ochrany utajovaných informací v informačních a komunikačních systémech:

- Vývoj v oblasti propojování informačních systémů s rozdílnými bezpečnostními požadavky na zabezpečení informací,
- vývoj v oblasti bezpečného využití virtualizačních nástrojů v informačních systémech,
- vývoj v oblasti definované bezpečnostním standardem NBÚ 1/2012 o opětovném užití, snížení a zrušení stupně utajení z moderních nosičů informací,
- vývoj nových metod zajišťujících adekvátní ochranu utajovaných informací stupně utajení Důvěrné a vyšší před jejich možným únikem kompromitujícím vyzařováním.

2.3 Prioritní výzkumná témata v oblasti kryptografické ochrany a vývoje kryptografických prostředků:

- Vývoj a analýzy národně jedinečných kryptografických algoritmů (primitiv, schémat a protokolů) pro ochranu utajovaných informací,
- adaptace a zkoumání možností využití mezinárodních kryptografických algoritmů z prostředí NATO a EU (primitiv, schémat a protokolů) a interoperabilních protokolů pro ochranu utajovaných informací,
- vývoj a certifikace kryptografických prostředků pro ochranu utajovaných informací, případně informací kritické infrastruktury,
- testování a analýza veřejně publikovaných kryptografických algoritmů a jejich implementací,
- příprava kryptografické ochrany na kvantovou hrozbu – analýzy bezpečnosti a vhodnosti použití různých protiopatření a kvantově odolných algoritmů,
- vysokorychlostní šifrování dat a hardwarová akcelerace kryptografických prostředků,
- výzkum a vývoj kryptografické ochrany autenticity dat v prostředí IoT a senzorových sítí,
- hodnocení hrozeb a rizik, tvorba krizových scénářů a metodik v oblasti kryptografické ochrany,
- technologie zaručující bezpečný příjem signálu veřejně regulované služby satelitního systému Galileo.

3 Cíle rozvoje VaVaI v kybernetické a informační bezpečnosti

V této kapitole je identifikováno pět cílů rozvoje a konkrétní nástroje k jejich naplnění. Smyslem níže uvedených cílů je přispět k rozvoji výzkumného a inovačního prostředí v prioritních výzkumných tématech kybernetické a informační bezpečnosti. Plnění jednotlivých cílů bude hrazeno ze stávajícího rozpočtu NÚKIB na výzkum a vývoj. Je nicméně žádoucí, aby docházelo k postupnému navyšování finančního prostředků tak, aby bylo možné realizovat například zahraniční výzkumné mise z rozpočtu NÚKIB (viz cíl 5).

Tabulka: seznam cílů

Cíl 1 – Prioritní výzkumná témata budou součástí veřejných soutěží a výzev národních a mezinárodních programů podpory výzkumu, vývoje a inovací
Cíl 2 – Vyšší zapojení uživatelské komunity do systému podpory VaVaI v kybernetické bezpečnosti včetně posílení schopnosti zavádět výsledky do praxe.
Cíl 3 – NÚKIB jako informační a analytické zázemí v oblasti VaVaI v kybernetické bezpečnosti
Cíl 4 – Rozvinutá mezinárodní spolupráce
Cíl 5 – NÚKIB aktivním účastníkem společně prováděného výzkumu a vývoje v kybernetické bezpečnosti na úrovni EU

3.1 Cíl 1 – Prioritní výzkumná témata budou součástí veřejných soutěží a výzev národních a mezinárodních programů podpory výzkumu, vývoje a inovací

Výchozí stav:

NÚKIB doposud nedisponoval uceleným a veřejně dostupným seznamem výzkumných témat, které by byly prosazovány u orgánů státní správy, akademické obce a soukromé sféry s cílem zajistit jejich stabilní podporu a dostatečné financování na národní a mezinárodní úrovni[15].

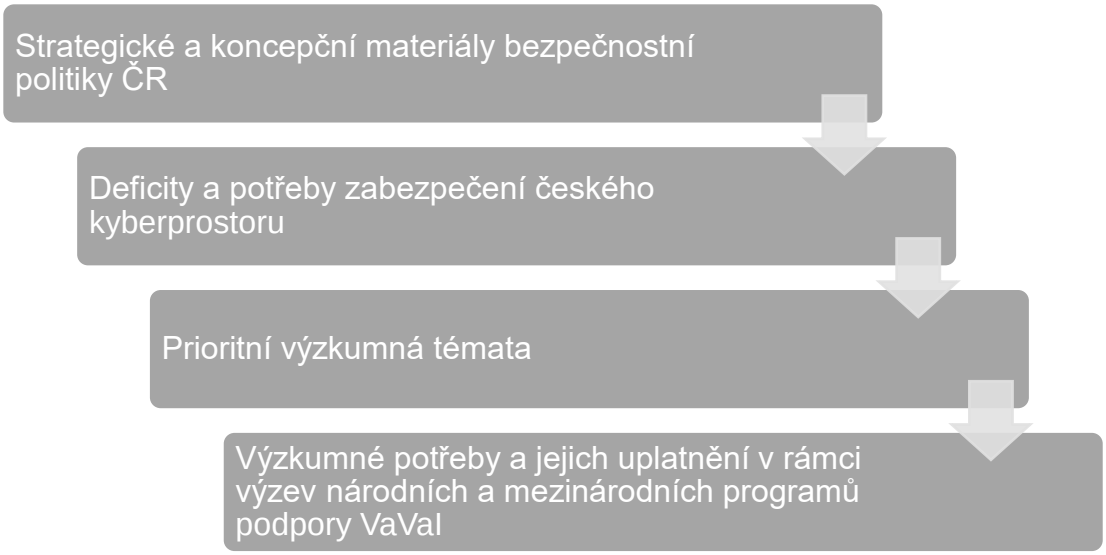
Nástroje:

- Na základě prioritních výzkumných témat NÚKIB vypracuje seznam výzkumných potřeb/cílů, včetně definice výzkumného cíle a popisu požadovaných výsledků. Seznam bude reflektovat deficity a potřeby zabezpečení českého kyberprostoru, včetně aktuálních bezpečnostních trendů (viz schéma). Prioritní výzkumná témata budou prosazována zejména v rámci programů podpory VaVaI v gesci:
    - Ministerstva vnitra ČR – Program bezpečnostního výzkumu České republiky v letech 2015 až 2022, Program bezpečnostního výzkumu pro potřeby státu 2016 - 2021, Strategická podpora rozvoje bezpečnostního výzkumu ČR 2019 – 2025 (IMPAKT 1),
    - Technologické agentury ČR – program BETA2,

[15] Výzkumná témata jsou také v souladu se strategickými prioritami v kybernetické bezpečnosti Agentury Evropské unie pro bezpečnost sítí a informací (ENISA), viz Analysis of the European R&D priorities in cybersecurity, European Cyber Security Organization – SRIA.

- Ministerstva pro místní rozvoj – Integrovaný regionální operační program pro období 2021 – 2027[16],
- Ministerstva průmyslu a obchodu – programy TREND a The Country for the Future,
- a dalších programů s přesahy do kybernetické a informační bezpečnosti.

Schéma: Systém identifikace výzkumných potřeb



3.2 Cíl 2 – Vyšší zapojení uživatelské komunity do systému podpory VaVaI v kybernetické bezpečnosti včetně posílení schopnosti zavádět výsledky do praxe.

Výchozí stav:

NÚKIB se podílí na realizaci několika projektů a s ohledem na jejich zaměření vystupuje v roli sponzora projektu, zadavatele veřejné zakázky či koncového uživatele odpovědného za nasazování nových technologií v praxi. NÚKIB zároveň úzce spolupracuje s příjemci veřejné podpory, dále také se specializovanými útvary Policie ČR a zpravodajských služeb zabývajících se kybernetickou kriminalitou. Tito aktéři disponují znalostí o potřebách praxe a jsou tak schopni posuzovat návrhy projektů z hlediska jejich společenské relevance. Je proto zapotřebí klást důraz na intenzivnější zapojování komunity uživatelů na různých rozhodovacích úrovních systému podpory VaVaI v kybernetické bezpečnosti.

[16] NÚKIB bude usilovat o opětovné vyhlášení výzvy „Kybernetická bezpečnost“, která byla vyhlášena v roce 2015 v rámci programového období 2014 – 2020.

Nástroje:

- NÚKIB bude iniciovat a podporovat zapojení komunity uživatelů do:
    - rad programů Ministerstva vnitra ČR a dalších poskytovatelů veřejné podpory na VaVaI,
    - databází oponentů MV, TA ČR a MPO,
    - kontrolní činnosti při realizaci projektů,
    - příslušných orgánů programů Horizont 2020, Horizont Evropa a Digitální Evropa,
    - národních a mezinárodních programových iniciativ.

- Pravidelná analýza a sběr informací o aktuálních potřebách konečných uživatelů prostřednictvím nově vytvořené Platformy k výzkumu a vývoji v kybernetické a informační bezpečnosti, jejímiž hlavními úkoly budou:
    - zajistit synergie mezi výzkumnými schopnostmi akademické obce a potřebami koncových uživatelů působících v kybernetické bezpečnosti,
    - zmapovat nároky kladené na uplatnění produktů na trhu,
    - hledat společná zájmová témata a zabránit výzkumným překryvům,
    - zprostředkovat přenos výsledků VaVaI k potenciálním výrobcům a koncovým uživatelům,
    - vyhodnocovat stav národní a mezinárodní spolupráce v oblasti VaVaI,
    - vyhodnocovat aktuální technologické trendy v kybernetické bezpečnosti a zajistit vzájemnou informovanost jednotlivých aktérů.

- NÚKIB podpoří vznik Digitálních inovačních hubů a dalších platforem, kde dochází k transferu výsledků výzkumu do praxe.

3.3 Cíl 3 – NÚKIB jako informační a analytické zázemí v oblasti VaVaI v kybernetické bezpečnosti

Výchozí stav:

V současnosti existuje řada různých informačních nástrojů zprostředkovávajících informace o národních a mezinárodních výzkumných programech. Informace však nejsou koncentrovány do jednoho informačního zdroje, tematicky se nezaměřují výhradně na problematiku kybernetické bezpečnosti a plně tak neslouží expertům v oblasti kybernetické bezpečnosti. Je proto žádoucí vytvořit na stránkách NÚKIB informační zdroj, kde zájemce nalezne informace o rámcových programech EU, aktuálních programových výzvách v oblasti kybernetické

bezpečnosti či návodný postup zapojení do mezinárodních konsorcií. Součástí rozvoje informačního zázemí bude i sledování a analýza aktuálních trendů v kybernetické a informační bezpečnosti s cílem poskytnout partnerům zajímavé informace o nových technologiích a bezpečnostních výzvách.

Nástroje:

- Vytvořit a pravidelně aktualizovat záložku „výzkum“ na internetových stránkách NÚKIB,
- šestkrát ročně NÚKIB rozešle partnerům zpravodaj s aktualitami na poli VaVaI v kybernetické bezpečnosti, který zároveň umístí na web,
- zástupce NÚKIB se v rámci finančních možností účastní síťovacích akcí pořádaných Evropskou komisí a dalšími orgány EU ve snaze usnadnit účast českých subjektů v mezinárodních konsorciích evropského výzkumného programu Horizont 2020, resp. Horizont Evropa a Digitální Evropa či Fondu pro vnitřní bezpečnost (ISF) a Nástroje pro propojení Evropy (CEF),
- NÚKIB připraví seznam národních a mezinárodních kontaktů, na základě kterého bude partnery oslovovat s nabídkou účasti v relevantních výzkumných projektech,
- NÚKIB každý měsíc zašle partnerům monitoring otevřených zdrojů zaměřený na technologické trendy v rámci prioritních výzkumných témat,
- NÚKIB zpracuje souhrnnou Zprávu o trendech v kybernetické a informační bezpečnosti, jejíž výstupy mohou být mimo jiné využity jako podklad pro další směřování podpory VaVaI a stanovení aktuálních prioritních výzkumných témat. Zpráva bude vytvořena za využití vlastních zdrojů NÚKIB.

3.4 Cíl 4 – Rozvinutá mezinárodní spolupráce

Výchozí stav:

Zahraniční spolupráce s sebou přináší nejen přístup k zahraničnímu know-how, ale také otvírá cestu k diverzifikaci zdrojů financování výzkumných aktivit. V ČR existuje řada špičkových výzkumných pracovišť a podniků, pro které je mezinárodní výzkumná spolupráce běžnou součástí jejich fungování. Úspěšnost zapojení českých subjektů do projektů financovaných z evropských výzkumných programů je však stále nízká[17]. NÚKIB v tomto může pomoci s vytvářením podmínek k rozvoji kontaktů se špičkovými zahraničními pracovišti a zároveň podporovat výzkumnou komunitu vlastní účastí v mezinárodních projektech.

[17] Frank, D., Albrecht, V. (2016): Účast ČR v H2020 a v programu Euratom v období leden 2014 – květen 2017, ECHO, 2016, příloha 3-4/2016, 34 s.

Nástroje:

- NÚKIB podpoří vznik mezinárodních konsorcií a s ohledem na vnitřní kapacity NÚKIB se zapojí do mezinárodních projektů, jejichž výsledky mají potenciál přispět k rozvoji ochrany českého kyberprostoru,
- ve spolupráci s kyber-atašé, vědeckými diplomaty a zastupitelskými úřady v zahraničí NÚKIB organizuje zahraniční výzkumné mise s cílem navázat dlouhodobou strategickou spolupráci s předními pracovišti v zahraničí. V průběhu přípravy tematického zaměření misí bude NÚKIB spolupracovat s MV a MO s cílem soustředit podporu do prioritních výzkumných témat kybernetické bezpečnosti,
- NÚKIB bude nadále zajišťovat podporu plnění závazků plynoucích z mezinárodních úmluv a z členství ČR v odborných skupinách a organizacích mezinárodního charakteru působících v oblasti VaVaI v kybernetické a informační bezpečnosti,
- NÚKIB se aktivně účastní společně prováděného výzkumu a vývoje v kybernetické a informační bezpečnosti na úrovni NATO.

3.5 Cíl 5 – NÚKIB aktivním účastníkem společně prováděného výzkumu a vývoje v kybernetické bezpečnosti na úrovni EU

Výchozí stav:

V současnosti probíhají intenzivní jednání na úrovni členských států EU o podobě rámcových programů v souvislosti s přípravou nového programového období 2021 – 2027. EU rovněž zvyšuje svou kapacitu týkající se ochrany členských států před stále častějšími kybernetickými hrozbami a zahájila přípravu nové struktury ke sdružování a vytváření sítí svých odborných znalostí v různých oblastech kybernetické bezpečnosti. Z hlediska národní pozice NÚKIB v oblasti kybernetické bezpečnosti je přirozené, že NÚKIB bude zastávat aktivní roli při formování nových rámcových programů EU a ve spolupráci s dalšími resorty bude podporovat národní iniciativy směřující k aktivnější roli ČR při zvyšování odolnosti EU vůči kybernetickým hrozbám.

Nástroje:

- NÚKIB bude prosazovat prioritní výzkumná témata do výzev programů Horizont Evropa a Digitální Evropa,

- podpora vzniku Národního koordinačního centra v ČR v souvislosti s návrhem nařízení zřídit Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center[18],
- NÚKIB podpoří vznik Evropského centra excelence v AI na území ČR, které se mj. bude zaměřovat na kybernetickou bezpečnost AI produktů, služeb a procesů a také na prevenci zneužití AI technologií,
- NÚKIB bude posilovat spolupráci s dalšími zahraničními organizacemi, které mají vliv na směřování výzkumu a vývoje na úrovni EU (například Evropská organizace pro kybernetickou bezpečnost – ECSO či Agentura Evropské unie pro bezpečnost sítí a informací – ENISA),
- NÚKIB bude spolupracovat s dalšími orgány státní správy v rámci Politiky soudržnosti EU,
- NÚKIB posílí spolupráci s delegátem programového výboru Horizont 2020 (resp. Horizont Evropa), národními kontaktními body a styčnými kancelářemi pro výzkum, vývoj a inovace v Bruselu.

4 Řízení rizik – omezení a předpoklady

Klíčovým předpokladem pro naplnění většiny výše uvedených cílů je dostatečné personální zajištění NÚKIB. Nedostatek kvalifikovaného personálu může vést k utlumení některých aktivit, a to především v oblasti mezinárodní spolupráce či vytváření informačního zázemí. Dále je nezbytné přinejmenším zachovat dosavadní míru alokovaných finančních prostředků na výzkum a vývoj a další podpůrné aktivity. V krátkodobém a střednědobém horizontu je žádoucí navyšovat finanční prostředky, které budou využity například na zajištění účasti pracovníka NÚKIB na jednáních projektového týmu v zahraničí (v případě zapojení NÚKIB do mezinárodního projektu) či na realizaci zahraničních výzkumných misí. V případě nedostatku finančních zdrojů bude nutné zajistit realizaci zahraničních výzkumných misí ve spolupráci s jinými resorty, například s MV, MO či MZV.

Dále je zapotřebí vhodně nastavit spolupráci s dalšími resorty a tuto spolupráci dále prohlubovat. Úspěšná realizace některých opatření je odvislá od společného postupu a v případě jeho selhání hrozí zásadní nedostatky při realizaci konkrétních opatření.

Dalším externím omezením je periodicita vyhlašování programů veřejné podpory a příslušných výzev. V případě vyčerpání alokovaných finančních prostředků nemusí být v roce 2020 vyhlášeny nové výzvy, čímž se zásadně omezí schopnost plnit opatření v cílech 1 a 2.

[18] Návrh Nařízení Evropského parlamentu a Rady, kterým se zřizuje Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center.

Analogická situace může nastat i na úrovni struktury a implementace nových programů EU či ve způsobu nastavení podmínek pro žadatele finanční podpory. NÚKIB má v tomto směru omezené možnosti, jak těmto rizikům předcházet. Jedním ze způsobů je aktivní účast NÚKIB při vytváření priorit pro VaVaI v ČR a v zahraničí či úzká spolupráce s gestory jednotlivých výzkumných programů.

5 Výhled do roku 2023

Po skončení platnosti tohoto Národního plánu, tedy po roce 2020, lze předpokládat, že proběhne vyhodnocení zkušeností z nových postupů, které tento plán zavádí. Bude vyhodnocena schopnost NÚKIB plnit stanovené cíle a také zda jsou prioritní výzkumné oblasti, s ohledem na dynamiku vývoje kybernetických hrozeb, stále aktuální. Vliv na VaVaI v kybernetické a informační bezpečnosti bude mít také nastavení nového programového období 2021 – 2027 a vývoj podpory VaVaI z národních zdrojů. Následující Národní plán pro období 2021 – 2022 bude vypracován v úzké vazbě s Národní strategií kybernetické bezpečnosti ČR na období let 2021 až 2025.

6 Plán plnění cílů

CÍL	NÁSTROJ	INDIKÁTOR	PROVÁDÍ	SPOLUPRACUJE S	PROJEDNÁ S	TERMÍN PLNĚNÍ
1	Vypracování seznamu výzkumných potřeb/cílů, včetně definice výzkumného cíle a popisu požadovaných výsledků. Seznam bude reflektovat deficity a potřeby zabezpečení českého kyberprostoru včetně aktuálních bezpečnostních trendů	seznam výzkumných potřeb/cílů	NÚKIB	Policie ČR, BIS, VZ, ÚZSI	MV, MO, MŠMT, MPO, TAČR, MMR, RVVI	2020
		zvyšující se počet realizovaných projektů se zaměřením na prioritní výzkumná témata oproti minulému roku				2020
2	Zapojení komunity uživatelů do: • rad programů Ministerstva vnitra ČR a dalších poskytovatelů veřejné podpory na VaVaI, • databází oponentů MV ČR, TA ČR a MPO, • kontrolní činnosti při realizaci projektů, • příslušných orgánů programů Horizont Evropa a Digitální Evropa, • národních a mezinárodních programových iniciativ Pravidelná analýza a sběr informací o aktuálních potřebách konečných uživatelů prostřednictvím nově vytvořené Platformy k výzkumu a vývoji v kybernetické a informační bezpečnosti NÚKIB podpoří vznik Digitálních inovačních hubů a dalších platforem, kde dochází k transferu výsledků výzkumu do praxe.	zvyšující se počet uplatněných expertů	NÚKIB	Policie ČR, BIS, VZ, ÚZSI a další externí partneři	MV, MO, MŠMT, MPO, TAČR, MMR, RVVI	2020
		zřízení a 2x ročně setkání Platformy k výzkumu a vývoji v kybernetické a informační bezpečnosti				2019 – 2020
				akademická a soukromá sféra	MPO, MŠMT, MMR	2020
3	Vytvořit a pravidelně aktualizovat záložku výzkum na internetových stránkách NÚKIB	vznik záložky webu	NÚKIB	TC AV ČR		průběžně

	Vypracovat zpravodaj s aktualitami na poli VaVaI v kybernetické bezpečnosti	6x ročně zpravodaj s aktualitami na poli VaVaI				2019 – 2020
	Účast na síťovacích akcí pořádaných Evropskou komisí			TC AV ČR	akademická a soukromá sféra	2019 – 2020
	NÚKIB připraví seznam národních a mezinárodních kontaktů, na základě kterého bude partnery oslovovat s nabídkou účasti v relevantních výzkumných projektech	průběžně aktualizovaný seznam národních a mezinárodních kontaktů				průběžně
	NÚKIB každý měsíc zašle partnerům monitoring otevřených zdrojů zaměřený na technologické trendy v rámci prioritních výzkumných témat	12x ročně monitoring otevřených zdrojů				2019 – 2020
	NÚKIB zpracuje souhrnnou Zprávu o trendech v kybernetické a informační bezpečnosti, jejíž výstupy mohou být mimo jiné využity jako podklad pro další směřování podpory VaVaI a stanovení aktuálních prioritních výzkumných témat.	1x ročně Zpráva o trendech v kybernetické a informační bezpečnosti			akademická a soukromá sféra	2020
4	NÚKIB podpoří vznik mezinárodních konsorcií a s ohledem na vnitřní kapacity NÚKIB se zapojí do mezinárodních projektů, jejichž výsledky mají potenciál přispět k rozvoji ochrany českého kyberprostoru,	zvyšující se počet podaných projektových žádostí společně se zahraničním partnerem	NÚKIB	akademická a soukromá sféra, TC AV ČR	Policie ČR, BIS, VZ, ÚZSI a další externí partneři	průběžně
	Realizace zahraničních výzkumných misí	2x ročně výzkumná mise včetně následného vyhodnocení přínosů misí		MV, MO, MZV		2020
	Podpora plnění závazků plynoucích z mezinárodních úmluv				MZV	průběžně
	NÚKIB se aktivně účastní společně prováděného výzkumu a vývoje v kybernetické a informační bezpečnosti na úrovni NATO			MO, VZ		průběžně

5	Prosazovat prioritní výzkumná témata do výzev programů Horizont 2020, Horizont Evropa a Digitální Evropa	Prioritní výzkumná témata součástí programů Horizont Evropa a Digitální Evropa	NÚKIB	MŠMT, ÚV, MPO	Policie ČR, BIS, VZ, ÚZSI, akademická a soukromá sféra	2020
	Podpora vzniku Národního koordinačního centra v ČR v souvislosti s návrhem nařízení zřídit Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center	Vznik Národního koordinačního centra	NÚKIB	ÚV, MŠMT, MF, MPO		2020 – 2021
	Podporovat vznik Evropského centra excelence v AI na území ČR		NÚKIB	MPO, ÚV, MŠMT, MD		2020 – 2021
	Posilovat spolupráci s dalšími zahraničními organizacemi, které mají vliv na směřování výzkumu a vývoje na úrovni EU		NÚKIB	akademická a soukromá sféra, TC AV ČR		průběžně
	Spolupracovat s dalšími orgány státní správy v rámci Politiky soudržnosti EU		NÚKIB	MMR, MV		průběžně
	Úzce spolupracovat s delegátem programového výboru Horizont 2020, resp. Horizont Evropa		NÚKIB	MŠMT		průběžně

7 Seznam zkratek

CEF – Nástroj pro propojení Evropy

ECSO – Evropská organizace pro kybernetickou bezpečnost

ENISA – Agentura Evropské unie pro bezpečnost sítí a informací

EU – Evropská unie

ISF – Fond pro vnitřní bezpečnost

KII – Kritická informační infrastruktura

MD – Ministerstvo dopravy

MMR – Ministerstvo pro místní rozvoj

MO – Ministerstvo obrany

MPO – Ministerstvo průmyslu a obchodu

MŠMT – Ministerstvo školství, mládeže a tělovýchovy

MV – Ministerstvo vnitra

MZV – Ministerstvo zahraničních věcí

NATO – Severoatlantická aliance

NBÚ – Národní bezpečnostní úřad

NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost

RVVI – Rada pro výzkum, vývoj a inovace

TA ČR – Technologická agentura ČR

TC AV ČR – Technologické centrum Akademie věd ČR

ÚV – Úřad vlády ČR

VaVaI – Výzkum, vývoj a inovace

VIS – Významné informační systémy