# Otevřené výzvy v bezpečnostním výzkumu 2023-2029 (OPSEC)

Praha 2021

## Obsah

# 1 Identifikační údaje

## 1.1 Název programu

Otevřené výzvy v bezpečnostním výzkumu 2023 – 2029 (Open Calls for Security Research – OPSEC, dále jen „Program“).

## 1.2 Právní rámec programu

Program, realizovaný formou veřejných soutěží ve výzkumu, experimentálním vývoji a inovacích, je zpracován v souladu s platnou právní úpravou ČR, zejména dle zákona č. 130/2002 Sb., o podpoře výzkumu, experimentálního vývoje a inovací z veřejných prostředků a o změně některých souvisejících zákonů (zákon o podpoře výzkumu, experimentálního vývoje a inovací), ve znění pozdějších předpisů (dále jen „Zákon“) a dle Rámce Společenství pro státní podporu výzkumu, vývoje a inovací - Úřední věstník Evropské unie číslo 2014/C 198/01-29 (dále jen „Rámec“).

Program bude dále realizován podle Nařízení Komise (EU) č. 651/2014 ze dne 17. června 2014 (GBER) (ve znění novely – Nařízení Komise č. 1084/2017, Nařízení Komise č. 972/2020 a Nařízení Komise č. 452/2021), kterým se v souladu s články 107 a 108 Smlouvy prohlašují určité kategorie podpory za slučitelné s vnitřním trhem – Úřední věstník Evropské unie L 187, 26. června 2014 (dále jen „Nařízení“), zejm. čl. 25, 28 a 29; a podle ostatních souvisejících předpisů.

Program je vyňat z oznamovací povinnosti podle čl. 108 odst. 3 Smlouvy o fungování Evropské unie, neboť splňuje podmínky Nařízení.

## 1.3 Identifikační kód programu

Pro účely evidence v Informačním systému výzkumu, experimentálního vývoje a inovací byl Programu přidělen identifikační kód „VK“.

## 1.4 Doba trvání a termíny vyhlášení programu

Termín vyhlášení Programu: **1. 1. 2023.**

Doba trvání Programu: 7 let, tj. do **31. 12. 2029.**

Programy veřejné soutěže mají v systému účelové podpory bezpečnostního výzkumu stabilizační úlohu, proto je doba realizace Programu 7 let, přičemž platí, že délka projektů nepřekročí 4 roky, aby nedocházelo ke snižování bezpečnostního přínosu z výsledků. Délka programových projektů je proto stanovena na 24–48 měsíců. Základním nástrojem realizace Programu je jednostupňová veřejná soutěž. Vzhledem ke specifickému charakteru bezpečnostního výzkumu předpokládá poskytovatel možnost využití dalších instrumentů Zákona v podobě dvoustupňové soutěže nebo postupu podle § 7 odst. 4, resp. § 17 odst. 4 Zákona**. Vyhlášení 1. veřejné soutěže se předpokládá v roce 2022. Celkově se v Programu předpokládá vyhlášení minimálně 3 veřejných soutěží. Poskytovatel předběžně předpokládá vyhlášení dalších soutěží v letech 2024 a 2025.**

## 1.5 Kategorizace charakteru výzkumu

Program podporuje projekty, které mají charakter aplikovaného výzkumu nebo experimentálního vývoje. Předmětem výzkumu mohou být i utajované informace a zvláštní skutečnosti podle zvláštních právních předpisů[1]. Podmínky k získání finanční podpory budou podrobně popsány v zadávací dokumentaci jednotlivých veřejných soutěží Programu a v návazných dokumentech.

[1] Pokud projekt i žadatel splňují požadavky zákona č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti a projekt svým věcným zaměřením spadá do některé z oblastí vymezených nařízením vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací, ve znění pozdějších předpisů, resp. projekt naplňuje charakteristiky „zvláštních skutečností“ významných pro krizové řízení ve smyslu §27 zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon).

Program bude podporovat 3 charakteristické typy projektů, odpovídající rozdílné očekávané vyspělosti výsledků. Blíže viz kap. 6.

## 1.6 Poskytovatel

Poskytovatelem veřejné podpory v rámci Programu je Ministerstvo vnitra.

# 2 Poslání a odůvodnění programu

Bezpečnostní výzkum představuje svébytnou agendu na pomezí vědní a bezpečnostní politiky, přičemž z hlediska každé z nich má široký potenciál, ale také významné limity. Obsahem této kapitoly je proto objasnění pozice Programu v portfoliu programových nástrojů Ministerstva vnitra, vymezení vůči obdobným programovým nástrojům ostatních poskytovatelů a identifikace vazeb a přínosů pro plnění cílů, stanovených strategickými dokumenty bezpečnostní a vědní politiky. Vlastní cíle Programu jsou uvedeny v kapitole 3.

## 2.1 Poslání programu

Posláním Programu je podpořit výzkumné a vývojové aktivity v oblasti bezpečnosti státu a jeho občanů v souladu s charakteristickými potřebami bezpečnostního systému a společenskými potřebami systémového charakteru v oblasti bezpečnosti, jak je vymezují platné strategické a koncepční materiály bezpečnostní politiky, které shrnuje Meziresortní koncepce podpory bezpečnostního výzkumu ČR 2017–2023[2] (dále jen „MKBV2017+“). Zároveň je Program nástrojem plnění Národní politiky výzkumu, vývoje a inovaci 2021+[3] (dále jen „NP VaVaI“). Program svou cílovou skupinou a zaměřením dále přispívá k plnění deklarovaných ambicí Inovační strategie ČR[4]. Sekundárně naplňuje i další strategické a koncepční dokumenty jako je např. Národní strategie umělé inteligence v ČR ( dále jen „Strategie AI“).

Program plní v portfoliu nástrojů podpory bezpečnostního výzkumu, experimentálního vývoje a inovací (dále jen „bezpečnostní výzkum“) páteřní roli. Jde o třetí generaci základního nástroje celého systému. I v třetí generaci je podpora otevřené soutěže relevantní, protože charakteristiky trhu bezpečnostních inovací se dlouhodobě příliš nemění. S tím je spojená potřeba mainstreamingu bezpečnostních témat v inovační sféře.

Trh bezpečnostních inovací je charakteristický především vysokou mírou fragmentace (především v evropském kontextu) dominantní rolí veřejných subjektů v roli konečných uživatelů – zákazníků, širokým spektrem relevantních problematik, které generují vysoce specializované požadavky na nasazované technologie, vysokou mírou konzervativismu v přístupu k akvizicím a obecně ke strategickému rozvoji, ve kterém navíc (min v celoevropském měřítku) v podstatě chybí dlouhodobý výhled a plánování schopností. V několika aspektech se tento segment liší i od obranného trhu. Jde o trh, kde je investice do vývoje vysoce riziková, zvláště u specializovaných inovací.

Kromě specifické oblasti kyberbezpečnosti a v některých velmi omezených segmentech také CBRN ochrany nejde o trh svébytný, charakteristický specializovanými dodavateli (mj. z výše uvedeného důvodu vysoké rizikovosti). Uvedené problematiky se vymykají obecnému trendu především proto, že reprezentují typické příklady dvojího užití, civilního bezpečnostního, stejně tak vojenského. Hlavní roli v bezpečnostním průmyslu hrají podniky obranného průmyslu s adaptovanými technologiemi, v menší míře naopak firmy orientované na zcela civilní produkty, které ale mohou mít po modifikaci v bezpečnostní oblasti relevanci.

Uvedená rizikovost představuje zcela zásadní inovační bariéru, protože je takřka prohibitivní pro aktéry tzv. netradiční, kteří ale čím dál častěji mohou s jistou modifikací zajímavé bezpečnostní

[2] Usnesení vlády č. 509/2017, o Meziresortní koncepci podpory bezpečnostního výzkumu ČR 2017–2023 s výhledem do roku 2030
[3] Usnesení vlády č. č. 759/2020 k Národní politice výzkumu, vývoje a inovací České republiky 2021+
[4] Usnesení vlády č. 104/2019, o Inovační strategii České republiky 2019–2030

inovace nabídnout. Pro aktéry obranného průmyslu je přinejmenším demotivující, protože „zcivilňování“ vojenských technologií není, s ohledem na mnohdy až překvapivé rozdíly mezi uživatelskými potřebami, příliš ekonomicky efektivní. Z toho důvodu panuje v EU, USA i v řadě dalších zemí (viz. „Současný stav zajišťování BV v ČR i v zahraničí“) konsensus, že efektivní bezpečnostní inovace mohou být motivovány pouze s aktivním zapojením státu.

Zároveň zajišťování bezpečnosti je stále více a více záležitostí technologickou. Rapidní růst závislosti společnosti na technologiích prakticky ve všech sférách moderního života přinesl zásadní změny také v hrozbách, kterým společnost tradičně čelí. V oblasti kriminality a organizovaného zločinu jde o trend zvlášť patrný, protože jde o oblast lidské činnosti takřka stejně dynamickou v aplikaci inovací, jako ostatní sektory legální ekonomiky. Obdobně současné hrozby, jako masová nelegální migrace, terorismus nebo hrozby tzv. hybridního charakteru mají svou zásadní technologickou dimenzi, stejně jako boj proti nim. Technologie také přináší zcela nové možnosti efektivnějšího řešení méně dynamických, ale mnohdy stejně závažných hrozeb přírodního původu, jejichž význam podtrhují klimatické změny. Na pomezí obou těchto celků potom stojí průmyslové havárie a selhání klíčových technologií v průmyslu.

Je tedy zřejmé, že i bezpečnostní sektor se může velmi efektivně rozvíjet v případě, že budou adekvátní inovace dostupné. Dosavadní konzervativní pojetí reakce na novou dynamiku hrozeb v podobě navýšení personálních stavů a stavů techniky již nemůže (minimálně v reakci na řadu závažných hrozeb) dostačovat. Poptávka se ale míjí s nabídkou.

Přestože Program jednoznačně směřuje ke snižování rizikovosti zapojení do segmentu bezpečnostních technologií, nebude pro účastníky a priori zdrojem zisku nebo uvedení produktu na trh. Návrh Programu daleko více akcentuje rozvoj znalostní a technologické základny. Proto podporuje především projekty ověřující nadějné technologické koncepty a jejich následný rozvoj směrem k prototypům. Pilotní nasazování a integrační aktivity jsou potom součástí jiných programových nástrojů. Program by tak měl umožnit zájemcům o bezpečnostní trh především udržet se na technologické špičce, než inkrementální inovace produktů.

Z hlediska věcného vymezení se Program snaží o maximální otevřenost, ale přesto zachovat moderační vliv. Program proto reflektuje relativně široké zájmové pole vycházející z koncepčních a strategických dokumentů bezpečnostní politiky, tak i z priorit MKBV2017+. Toto vymezení umožňuje variabilitu zaměření jednotlivých veřejných soutěží, stejně jako operativní reakci v případě identifikace nyní neznámých bezpečnostních hrozeb či dalšího vývoje koncepčních a strategických záměrů v bezpečnostní oblasti. [5] Program proto akcentuje především inovační potřeby bezpečnostních sborů, které jsou zároveň koncovými uživateli a které představují klíčový prvek implementace ve všech fázích od specifikace inovačních potřeb (viz zájmové pole z koncepčních a strategických dokumentů bezpečnostní politiky), přes možnost konzultace a testování průběžných řešení až po implementaci v praxi. Tato pevnější vazba je taktéž přínosem *pro excelentní výzkum*.

## 2.2 Pozice Programu v portfoliu programových nástrojů Ministerstva vnitra

V souladu s MKBV2017+ tvoří portfolio bezpečnostního výzkumu čtyři komplementární programy účelové podpory, zaměřené na odlišné typy aktivit. Pokrývají celou škálu od vývoje konceptu řešení po testování a evaluaci výsledků za reálných podmínek nasazení. Jsou to tyto programy:

**Program bezpečnostního výzkumu České republiky v letech 2015 až 2022 (VI)**, jehož posláním je podpořit výzkumné a vývojové aktivity v oblasti bezpečnosti státu a jeho občanů v souladu se strategií prevence, minimalizace a potlačování bezpečnostních hrozeb, stanovenou Bezpečnostní

[5] viz například zohlednění závěrů Auditu národní bezpečnosti v rámci 3. veřejné soutěže Programu bezpečnostního výzkumu ČR v letech 2015 až 2022 (Program VI) či rychlá reakce na pandemickou krizi vyhlášením 4. veřejné soutěže, zaměřené na řešení epidemiologických hrozeb, v rámci téhož programu.

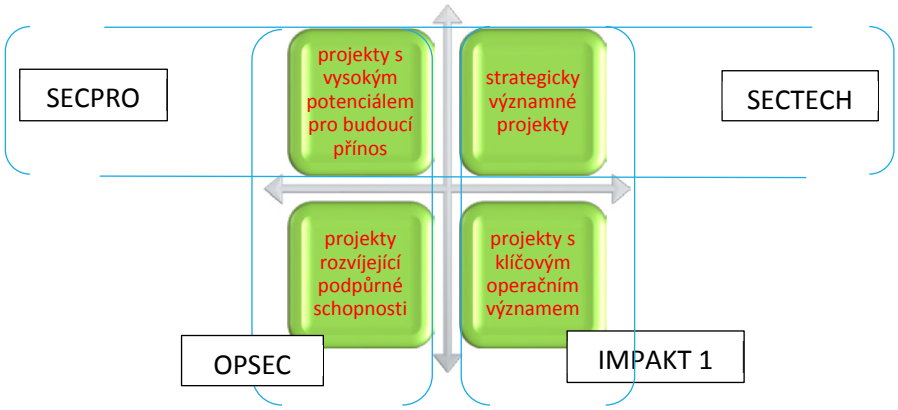
strategií ČR, Národními prioritami orientovaného výzkumu, experimentálního vývoje a inovací a prioritami Meziresortní koncepce bezpečnostního výzkumu a vývoje České republiky do roku 2015[6].

**Program bezpečnostního výzkumu pro potřeby státu v letech 2022-2027 (SecPro)**, který je určen k naplňování konkrétních výzkumných potřeb orgánů státní správy podílejících se na plnění úkolů v rámci systému vnitřní bezpečnosti a ochrany obyvatelstva ČR. Uživatelem výsledků programu je stát, tj. příslušný orgán státní správy, který své výzkumné potřeby předložil poskytovateli.

**Strategická podpora rozvoje bezpečnostního výzkumu ČR 2019-2025 (IMPAKT 1)**, tedy program, který vytváří podmínky pro využití a rozvoj potenciálu akademického a veřejného výzkumného sektoru, který zajišťuje synergickou a dlouhodobou výzkumnou podporu bezpečnostního systému ČR, včetně podpory mezinárodní spolupráce v bezpečnostním výzkumu.

**Program bezpečnostního výzkumu ČR 2021–2026: vývoj, testování a evaluace nových bezpečnostních technologií (SECTECH)**, jehož hlavním cílem je mobilizace potenciálu podnikového sektoru, zejm. začínajících, malých a středních podniků, k participaci na vývoji a transferu nových bezpečnostních technologií. SECTECH se záměrně soustředí na vysoké stupně technologické vyspělosti.

Programy se soustředí na čtyři druhy výzkumných projektů. V prvé řadě jsou to **strategicky významné** projekty, které se zaměřují na rozvoj schopností bezpečnostního systému, které mají dlouhodobě kritický význam z hlediska plnění jeho úkolů v budoucnu, s ohledem na trendy a vývoj bezpečnostního prostředí. Druhou nejvýznamnější skupinou by měly být projekty zaměřené na rozvoj schopností, které mají, vzhledem k vývoji bezpečnostního prostředí, **vysoký potenciál** pro budoucí přínos. Třetí skupinou jsou projekty zaměřené na **klíčové operační schopnosti**, tj. takové, které jsou v současnosti
i v budoucnu nutné k plnění poslání bezpečnostního systému. Projekty, které rozvíjí **podpůrné schopnosti** s významnou, nikoli však kritickou hodnotou, jsou v kategorizaci priorit nejméně významnou skupinou. Následující matice kategorizuje portfolio projektů napříč programy.




**Tabulka 1: Portfolio programů bezpečnostního výzkumu**

V souladu s výše uvedenými cíli a zaměřením je v jednotlivých programech adekvátně rozpracována řada individuálních charakteristik, od tematického zaměření na priority a oblasti bezpečnostního výzkumu vymezené v MKBV2017+, přes preferované druhy hlavních výsledků a jejich vlastnictví a přes zapojení uživatelských organizací do projektů v rolích aplikačních garantů a testovacích autorit včetně adekvátních výběrových, a hodnotících kritérií, které kladou důraz na odlišné atributy projektů i charakteristiky řešení.

[6] Návrh tohoto Programu navazuje na aktuálně realizovaný Program bezpečnostního výzkumu ČR v letech 2015 až 2022 (Program VI)

**Otevřené výzvy v bezpečnostním výzkumu 2023 – 2030 (OpSec)** je páteřním programem portfolia programových nástrojů účelové podpory bezpečnostního výzkumu. Navazuje na předchozí úspěšný Program bezpečnostního výzkumu České republiky 2010 – 2015 (VG) a probíhající Program bezpečnostního výzkumu České republiky v letech 2015 až 2022 (VI). Spolu s programem bezpečnostního výzkumu pro potřeby státu (SecPro) představuje Program základní operační schopnosti systému podpory bezpečnostního výzkumu a hladinu, ke které se systém může vracet v případě, že nebude dostatečně finančně saturován. Program navazuje na analýzu minulých zkušeností, na potřeby, stav a požadavky kladené na systém bezpečnostního výzkumu, které shrnuje MKBV2017+ a na aktuální potřeby bezpečnostního systému, vycházející z aktualizace relevantních strategických dokumentů po vstupu MKBV2017+ v platnost.

Prostřednictvím takto vytvořeného prostředí komplementárních podpůrných nástrojů účelové podpory, doplněné o podporu institucionální, je zajišťována maximalizace přínosu podpory bezpečnostního výzkumu a postupně dosahováno předpokládaného cílového stavu dle MKBV2017+, spočívajícího v tom, že bezpečnostní výzkum ČR bude k rozvoji klíčových schopností bezpečnostního systému cíleně využívat kreativity a potenciálu výzkumné a inovační sféry, jeho jednotlivých součástí a komunit partnerů. Tento flexibilní systém specializovaných nástrojů podpory umožňuje zaměřit výzkumnou činnost na nejpodstatnější bezpečnostní výzvy a získávat pro ně nová řešení či iniciovat mezinárodní aktivity výzkumných týmů v oblasti bezpečnosti.

## 2.3 Vazba na opatření strategických dokumentů politiky výzkumu, vývoje a inovací

### 2.3.1 Národní politika výzkumu, vývoje a inovací

MV při přípravě programových nástrojů bezpečnostního výzkumu vychází z předpokladu, dle kterého jsou koncepce poskytovatelů nástroji plnění Národní politiky výzkumu, vývoje a inovací 2021+ (dále jen „NP VaVaI“). Programy, které koncepce definují, na NP VaVaI implicitně navazují. V případě Programu je to zejména návaznost na opatření NP VaVaI *č. 22*: **Rozvoj obranného a bezpečnostního výzkumu**
**s možností využití v civilních aplikacích** a opatření *č. 27*: **Redefinice Národních priorit orientovaného výzkumu, experimentálního vývoje a inovací s cílem zvýšení odolnosti české společnosti – podpora specifických výzkumných programů relevantních pro oblasti definovaných hrozeb s celospolečenským dopadem.** Zajišťování obrany a bezpečnosti patří mezi hlavní úlohy každého státu, které významně ovlivňuje jak rozvoj aplikovaného výzkumu, tak společenské změny. Podstata branně-bezpečnostní problematiky a značná exkluzivita státu (jako jejího garanta) vyžadují specifický přístup k tvorbě expertních vstupů dotčených politik.

Ze zkušeností předních českých výzkumných organizací zaměřených na průmyslovou (smluvní) výzkumnou spolupráci také plyne, že řadu situací usnadňuje podpora právě tohoto typu spolupráce. Program proto podporuje realizaci kolaborativních projektů. Lze jej proto považovat také za nástroj plnění opatření NP VaVaI *č. 20*: **Podpora dlouhodobé spolupráce ve VaVaI mezi výzkumnými organizacemi a podniky a uplatnění společných výsledků aplikovaného výzkumu v praxi.**

V rámci portfolia bezpečnostního výzkumu je Program zaměřen na řadu dalších opatření NP VaVaI. Komplexní programové portfolio bezpečnostního výzkumu totiž zahrnuje nástroje pro rozvoj lidských zdrojů, udržování partnerství se zahraničními partnery, ale i úzkou spolupráci s těmi místními (program IMPAKT) a méně i více specializovanou účelovou podporu, podél celé škály technologické vyspělosti, od aplikovaného výzkumu po velmi pokročilý vývoj (programy SOUTĚŽ, SecPro a SECTECH – viz výše).

Program se také podílí na realizaci opatření NP VaVaI *č. 21*: **Realizace Národní RIS3 strategie** a opatření *č. 25*: **Komplexní podpora rozvoje a využití umělé inteligence** (viz níže).

### 2.3.2 Inovační strategie

Inovační strategie je svým charakterem i logikou dokumentem výrazně obecnějším a hierarchicky vzato výše postaveným, než aby přímo ovlivňoval charakteristiky konkrétních programů podpory. Pro jeho efektivní fungování je nutné vytvářet průnik s posláním poskytovatelů a účelem jejich jednotlivých podpor. Přesto lze i Program vztáhnout ke dvěma cílům tohoto dokumentu, resp. jej vnímat jako součást souboru opatření k plnění této strategie. Jde o:

- cíl „posílit účelovou podporu institucí, jejichž výsledky se uplatňují v praxi“ a účelovou podporu aplikovaného společenskovědního výzkumu“ cestou „zapojování firem do projektů výzkumu s výzkumnými organizacemi při soukromém kofinancování“ (kap. Financování a hodnocení výzkumu a vývoje). Tomu odpovídá zaměření Programu na spolupráci akademické a podnikové sféry i důraz na uživatelsky podmíněné vlastnosti výsledků, které jsou v segmentu bezpečnostních technologií pro uplatnění v praxi klíčové. Kofinancování je dáno limity veřejné podpory podle evropské legislativy[7].
- cíl „podporovat zavádění výsledků aplikovaného výzkumu v oblasti transformativních technologií do praxe“ cestou „podpory ve výzvách národních programů VaVaI pro technologická řešení a inovace v oblasti automatizace, robotizace a umělé inteligence“ (kap. Digitální stát, výroba a služby). Tato témata jsou velmi podstatnou součástí předvídatelných inovací v oblastech vymáhání práva nebo krizového řízení, což jsou primární funkce státu[8].

### 2.3.3 Vazba na priority bezpečnostní politiky, RIS3 strategie a Národních priorit orientovaného výzkumu

Strategické dokumenty bezpečnostní politiky tvoří složitý relační (nikoliv hierarchický) systém. V rámci přípravy MKBV2017+ byla provedena analýza těchto relačních vztahů z 22 platných a relevantních dokumentů, které vznáší požadavky na bezpečnostní výzkum a/nebo definují inovační směry a priority. Z těchto dokumentů byla vytvořena mapa relačních vztahů 93 bezpečnostních hrozeb, kterým je věnována pozornost, a 94 inovačních potřeb.[9] Nestejná úroveň (míra detailu) nejen mezi dokumenty, ale i uvnitř sledovaných dokumentů, prakticky znesnadňuje rozumný výběr a přímé zahrnutí.[10]

**Výsledkem procesu obsahové analýzy je proto formulace prioritizovaného věcného vymezení bezpečnostního výzkumu, které prezentuje MKBV2017+,** a ve kterém jsou sjednoceny charakteristické požadavky napříč celým spektrem výše studovaných dokumentů.[11] V Programu se předpokládá financování projektů v plném spektru zájmových oblastí ze všech 3 prioritních cílů podpory bezpečnostního výzkumu:[12]

**Efektivní zásah** (cíl v prioritě řešení bezpečnostních incidentů)

Zasahující personál budoucnosti je schopen včas identifikovat hrozící nebezpečí nebo probíhající incident, zorientovat se v situaci a v nejkratším možném čase adekvátně a koordinovaně reagovat v jeho průběhu i po jeho skončení v souladu se svou systémovou funkcí. K tomu je všestranně připraven a vybaven vhodnými prostředky, včetně vlastní ochrany, které vždy splňují přísné nároky na funkci v náročných podmínkách a zároveň nesnižují úroveň pozornosti, či jinak nezatěžují fyzické či kognitivní kapacity jedince.

V rámci tohoto prioritního cíle jsou rozvíjeny následující zájmové oblasti:

[7] Jedná se odkaz na Inovační strategii na kapitolu zaměřenou na financování a hodnocení výzkumu a vývoje a na vytyčené cíle v tomto dokumentu.

[8] Viz poznámka pod čarou č. 7.

[9] Alespoň vzdáleně relevantních pro bezpečnostní výzkum, potřeby typu zvýšení rozpočtu nebo navýšení počtů personálu nebyly zahrnuty.

[10] Bezpečnostního výzkumu se na této úrovni navíc dotýkají i další dokumenty, jako např. strategie Průmysl 4.0, kterou materiál také zohledňuje.

[11] Na věcném vymezení bezpečnostního výzkumu, včetně jeho prioritních cílů panuje široký konsensus napříč zainteresovanými stranami, neboť se valná většina součástí bezpečnostního systému podílela na práci komise, která MKBV2017+ formulovala.

[12] Prioritní cíl 2 „Adaptabilní bezpečnostní systém“ nezahrnuje priority vhodné k realizaci v tomto Program.

- Včasná výstraha a situační přehled
- Efektivní intervence
- Vyšetřování incidentů

**Adaptabilní bezpečnostní systém** (cíl v prioritě rozvoj bezpečnostního systému)

Základem uvažování o bezpečnosti jsou prediktivní analýza, soustavná analýza rizik, modelování, simulace a evaluace. Bezpečnostní systém budoucnosti z nich těží a promítá jejich závěry do regulace i plánování na všech rozhodovacích úrovních. Jednotlivé bezpečnostní složky a součásti bezpečnostního systému se vnitřně vyvíjí a optimalizují vlastní plány, postupy, řídící procesy a náklady tak, aby byly vždy schopné plnit své úkoly v požadované kvalitě a rozsahu, a tyto aspekty aktivně maximalizovat učením se ze zkušeností. Jejich směřování probíhá proaktivně, v prostředí, kde kritická rozhodnutí podporují přesné, důvěryhodné a precizně analyticky zpracované informace z maximálního možného spektra relevantních zdrojů.

V rámci tohoto prioritního cíle jsou rozvíjeny následující zájmové oblasti:

- Bezpečnostní politika a krizové řízení
- Vnitřní schopnosti součástí bezpečnostního systému
- Management bezpečnostních informací

**Resilientní komunity** (cíl v prioritě snižování rizik a zvyšování odolnosti)

Kultura bezpečnosti proniká i do uvažování o službách, prostředí a společnosti. Prostor, společenství i jeho klíčové podpůrné systémy se proaktivně zapojují do opatření ke snižování rizik katastrof nebo protispolečenských jevů, přičemž si zachovávají značnou míru tolerance rizika. Rozvíjí se předpoklady pro zachování kontinuity služeb a přístupu k nim a respektu k základním společenským hodnotám a potřebám zranitelných skupin obyvatelstva v průběhu krizové situace nebo pod tlakem protispolečenských jevů. Infrastruktury a jejich kritické prvky i části veřejného prostoru jsou navrhovány a stavěny tak, aby odolávaly přírodním katastrofám, haváriím i projevům protispolečenského chování a umožňovaly flexibilní, kontrolované využití v době krizové situace a rychlou obnovu. Proaktivní bezpečnostní kontrola, jako prvek zvyšování odolnosti, je přizpůsobena dynamice pohybu osob a zboží, i standardům lidských práv a zachování důstojnosti jedince. Komunity zasažené závažným bezpečnostním incidentem jsou schopny se s nimi rychle a úspěšně vypořádat, včetně minimalizace okamžitých i dlouhodobých a chronických následků.

V rámci tohoto prioritního cíle jsou rozvíjeny následující zájmové oblasti:

- Bezpečný veřejný prostor
- Bezpečnost infrastruktur
- Environmentální bezpečnost

Program svým zacílením plně koresponduje s aktuální Národní RIS3 strategií, ve které je bezpečnostní výzkum jako nadresortní a multioborový nově obsahově akcentován v doménách výzkumné a inovační specializace a zároveň naplňuje také konkrétní společenskou výzvu „Zvýšená bezpečnostní rizika
a proměnlivost bezpečnostních hrozeb“, která spadá do gesce Ministerstva vnitra a má též vazbu na resortní programy podpory bezpečnostního výzkumu. Základním principem jednotlivých misí v této výzvě je cestou systematického využívání i budování výzkumných kapacit získávat a efektivně rozvíjet inovativní znalosti, metody a technologie, které umožňují bezpečnostnímu systému ČR a jeho zainteresovaným partnerům čelit současným i budoucím rizikům, která plynou z uvedených měnících se realit bezpečnostního prostředí. Mise v této společenské výzvě primárně cílí na prioritní cíle MKBV2017+, a to na Efektivní zásah a Adaptabilní bezpečnostní systém.

Národní priority orientovaného výzkumu jsou v tomto směru selektivní podmnožinou obou dokumentů, přičemž dominantní překryv lze shledat s MKBV2017+.

Podporovaná témata budou dále specifikována v návazných dokumentech, zejména v zadávacích dokumentacích k jednotlivým veřejným soutěžím. Specifikace umožňuje reagovat na silné stránky českého výzkumného prostředí a přiblížit program dalším strategickým iniciativám, které bezpečnostní výzkum a priori nezmiňují (např. Strategie AI).

## 2.4 Současný stav řešení problematiky bezpečnostního výzkumu v ČR a v zahraničí

Bezpečnostní výzkum, resp. snaha veřejných subjektů stimulovat vývoj a implementaci inovací v bezpečnostním sektoru se u nás, v EU i v USA vyvíjí na základě velmi podobných impulzů. Patří mezi ně nutnost reagovat na proměnlivé bezpečnostní hrozby, se zvláštním důrazem na velmi dynamický vývoj v oblasti vymáhání práva nebo vysoce specifické charakteristiky trhu bezpečnostních technologií a jeho aktérů.

Obecně lze viditelnou dynamiku této problematiky sledovat postupně od útoků 11/9/2001, přes rozsáhlé evropské povodně v roce 2003 až po teroristické útoky v Londýně a Madridu v roce 2007. Všechny tyto události postupně přinesly přesvědčení, že veřejný systém zajišťování bezpečnosti potřebuje lépe využívat moderních technologických možností a schopností domácího průmyslu. V tom směru se aktivizovaly zainteresované komunity v EU i v USA a postupně postoupily k organizaci prvních dedikovaných nástrojů podpory tvorby bezpečnostních inovací. V ČR se první programy sjednocené v působnosti MV začaly připravovat v návaznosti na tzv. reformu systému poskytovatelů v roce 2008, mj. i ve vazbě na evropské trendy. Od té doby prošly všechny tři systémy poměrně značnou evolucí.

V USA se postupně vytvořil systém nástrojů v působnosti *Dept. of Homeland Security* (DHS), v rámci Ředitelství pro vědu a technologie. Způsob, jakým američtí poskytovatelé definují programové nástroje je od ČR značně odlišný a nelze je tedy vzájemně přímo srovnávat. V americkém systému postupně začal dominovat prvek konečného uživatele, který definuje velmi detailní technologické záměry
a požadavky a na jejich základě spolupracuje s dodavatelskou komunitou. Přímo v působnosti DHS jsou programy pro utváření zájmu o relevantní problematiky v univerzitním prostředí, které financují především malé juniorní projekty a studie (*University Centers of Excellence*), dále programy na podporu spolupráce s malými a středními podniky (SBIR a STTR), a v neposlední řadě skautingové aktivity v Sillicon Valley. Ekvivalent otevřených soutěží reprezentují tzv. *Broad Agency Announcements*, tedy výzvy s relativně obecně vymezeným spektrem témat k podpoře. Alokace na tento systém je cca 600 mil USD ročně. To ovšem nebere v potaz řadu dalších vývojových aktivit jednotlivých ozbrojených sborů a dalších aktérů. DHS se cíleně snaží o spolupráci s průmyslem, zejm. s tzv. netradičními dodavateli, se kterými úzce spolupracuje na vývoji zcela specifických technologických řešení.

V EU směřoval vývoj od obecnějších a tematicky orientovaných výzev v prvních pracovních programech Sedmého rámcového programu (tehdy v působnosti DG GROW) směrem k větší specializaci a užší spolupráci s uživatelskou komunitou. Tuto evoluci demonstrovala jak organizační změna – přesun agendy bezpečnostního výzkumu do DG HOME, tak daleko intenzivnější zapojení konečných uživatelů do managementu programu. To má v současnosti 2 formy. Jednak jde o poradní roli, kterou vůči bezpečnostnímu výzkumu v EU vykonává *Protection and Security Advisory Group* (PASAG), dále potom o povinné zapojování uživatelů do některých typů podporovaných projektů. Ruku v ruce s touto transformací přichází také jiný přístup k formulaci výzev. Ty jsou v současnosti detailnější a cílově orientované (namísto původního velmi obecného tematického vymezení). Posledním trendem ve vývoji evropského pohledu na problematiku bezpečnostního výzkumu je

zahrnutí vývoje na základě inovační poptávky veřejného sektoru ve snaze o překonání problémů se zaváděním inovativních technologií do praxe.

V rámcovém programu *Horizon Europe* je agenda bezpečnostního výzkumu pevně ukotvena s dotací cca 200 mil EUR ročně v rámci pilíře 2 – Globální výzvy a konkurenceschopnost evropského průmyslu. Tyto prostředky jsou předurčeny k podpoře 4 typů projektů, mezi nimi *Research and Innovation Action* a *Innovation Action*, které se od sebe liší výslednou technologickou vyspělostí a také intenzitou podpory. I EU explicitně deklaruje vazbu mezi podporou bezpečnostního výzkumu a snahou o překonání některých inherentních charakteristik trhu bezpečnostních technologií a, alespoň verbálně, propojuje toto financování s podporou konkurenceschopnosti průmyslu.

Nejpozději od roku 2007 se také rozvíjí národní programy podpory bezpečnostního výzkumu v řadě evropských zemí, obvykle inspirovaných snahou vytvářet domácí zázemí budoucím žadatelům o podpory evropské. V současnosti takovými programy disponují Francie, Německo, Rakousko, Nizozemsko, Finsko, Španělsko, Polsko a nově mimoevropská Velká Británie. Relativně menší a spíše na vnitřní potřeby orientovanou podporou disponuje také Švédsko. Význam problematiky rozvoje bezpečnostních inovací si tak uvědomuje řada evropských zemí a ČR za nimi v tomto smyslu nijak nezaostává.

V ČR lze sledovat trendy do jisté míry podobné vývoji v EU. V tuto chvíli je postupně implementována 3. generace programů bezpečnostního výzkumu, která se dvou předchozích výrazně liší. Reprezentuje ale kvalitativně jiný stav. První a druhou generaci programů bezpečnostního výzkumu charakterizovala snaha o co nejširší pokrytí celého zájmového prostoru formou otevřených výzev, kde jsou projekty zcela formulovány cestou *bottom-up*. Vedle toho v obou generacích existuje prostor pro řešení výzkumných potřeb bezpečnostního systému, cestou veřejných zakázek.

Za tyto dvě generace se podařilo postupně vytvořit jádro komunity bezpečnostního výzkumu, které reprezentují především velké univerzity. V některých klíčových technologických oblastech, jako umělá inteligence, se podařilo vytvořit efektivní podpory vedoucí jak k bezpečnostním, tak civilním inovacím. Dlouhodobě se MV také významně podílí na poskytování účelové podpory v oblasti kyberbezpečnosti. V první generaci programů dominovalo České vysoké učení technické (ČVUT), v současnosti jeho roli postupně přebralo Vysoké učení technické v Brně (VUT), skrze Fakultu informačních technologií (FIT) a Fakultu elektrotechniky a komunikačních technologií (FEKT). Na druhou stranu hraje akademický sektor roli efektivního partnera u řady velmi aktuálních témat, jako jsou elektronické důkazy v trestním řízení. Okolo tohoto jádra se vytvořila komunita různě velkých (převážně malých a středních) podniků, které s akademickou sférou aktivně spolupracují. Svou základní roli – motivovat schopné aktéry k práci na bezpečnostních tématech – programy tohoto typu plní. Protože se ale nemění podstata bezpečnostního trhu, trvá potřeba systém podpory bezpečnostního výzkumu rozvíjet.

Ve třetí generaci se MV reaguje na podobné výzvy, jako jeho zahraniční partneři a do systému přidává cílené programy pro rozvoj schopností akademické sféry (IMPAKT) a pro přenos výsledků z jiných technologických domén, včetně možnosti dodatečné podpory na dokončení inovativních produktů v rámci testování a vyhodnocování se zapojením uživatele (SECTECH). Páteřními součástmi systému ale stále zůstávají programy zakázkové (SecPro) a především otevřené výzvy. Ty jsou nadále vzájemně komplementární, protože SecPro umožňuje dotažení a pilotní nasazení technologií podle potřeb konečných uživatelů, zatímco OPSEC přináší podporu především nižších a středních stupňů technologické vyspělosti. Znamená to, že jde o program, který investuje především do inovací budoucích a staví na investicích a schopnostech vybudovaných v rámci např. operačních programů.

Poskytovatel zároveň zohledňuje všechny trendy, spojené s managementem bezpečnostního výzkumu, zejm. ve vztahu s konečnými uživateli a nijak se nezříká snahy o podporu bezpečnostního průmyslu, včetně jeho netradičních aktérů. Trend vyšší specializace výzev potom reprezentuje jednak

vymezení podprogramů, které vychází z platných strategických dokumentů bezpečnostní politiky a z mezinárodních trendů, dále potom snaha specializovat jednotlivé programové výzvy. Program se tak přibližuje mezinárodně uznanému (avšak nikde zcela nerealizovanému) modelu relativně úzce vymezených výzev, které především identifikují problémy a mezery ve schopnostech uživatelské sféry, ale ponechávají zcela otevřený prostor pro návrhy řešení. Z praktického důvodu tento postup v českém prostředí reprezentuje především vymezení podprogramů na základě platných strategických dokumentů a témat v nich akcentovaných.

# 3 Cíl a přínosy programu

## 3.1 Hlavní cíl

Hlavním cílem Programu je systematicky podněcovat a rozvíjet zájem výzkumné a inovační sféry o zapojení do řešení bezpečnostních výzev pro moderní společnost a tvořit tak základnu pro rozvoj konkurenceschopných bezpečnostních inovací.

### 3.1.1 Dílčí cíle programu

Každý projekt by měl směřovat k výsledkům, jejichž budoucí nasazení v praxi má ve střednědobém horizontu potenciál přispět k plnění některého z následujících cílů:

1. zefektivnění plánování, koordinace a regulace (tj. zefektivnění přípravy na krizové situace/incidenty/společenské jevy);
2. zvýšení dostupnosti služeb bezpečnostního systému (tj. rozsahu nebo kvality či rychlosti reakce);
3. snížení ohrožení (tj. omezení pravděpodobnosti vzniku negativních dopadů krizové situace/incidentu/jevu);
4. zefektivnění včasného varování (zejména prodloužení doby na reakci, zvýšení spolehlivosti varování);
5. zvýšení bezpečnosti zasahujících, včetně vyšetřování a expertizní činnosti;
6. zvýšení efektivity činnosti zasahujících, včetně vyšetřování a expertizní činnosti;
7. zmírnění následků (tj. omezení intenzity a rozsahu dopadů krizové situace/incidentu/jevu).

## 3.2 Očekávané přínosy programu

Program se stane jedním ze stimulů k využívání potenciálu výzkumné kapacity ČR napříč oborovými skupinami pro řešení projektů bezpečnostního výzkumu a vývoje. Tím se Program zapojí do systému rozvoje bezpečnostních inovací. Protože je toto prostředí vysoce specifické a zároveň z pohledu „netradičního“ dodavatele vysoce rizikové, přinese Program odstranění některých inovačních bariér pro jejich zapojení. Vedle toho očekává poskytovatel – v návaznosti na zkušenosti z minulých generací programu – také sekundární přínosy pro zapojené organizace.

Program má ambice přinést:

Konečným uživatelům výsledků:

- kontakt s výzkumným a inovačním sektorem a tím větší přehled o technologických možnostech a trendech, včetně možnosti navázat na tyto trendy pokročilé projekty v komplementárních nebo akvizičních programech
- možnost ovlivnit zacílení podpory i směřování projektů, tedy posílit roli při určování kvalitativních požadavků na nové technologie a postupy
- nástroj pro aktivní využití schopností výzkumné a inovační sféry k reakci na rychle přicházející společenské a technologické trendy, které mají zásadní dopad na bezpečnostní prostředí

Výzkumníkům a inovátorům:

- nástroj pro bezrizikové financování konceptualizace a ověření potenciálních nových technologií
- výrazné snížení rizikovosti investice do vývoje inovativních bezpečnostních technologií
- interakci s uživatelem a přenos know-how, tím pádem vyšší kvalitu (relevanci) výsledků vedoucí k vyšší konkurenceschopnosti v tomto specifickém tržním segmentu, *což povede k podpoře excelentního výzkumu jako celku*
- sekundární přínosy pro organizaci příjemce (lidské zdroje – zapojení juniorních výzkumníků a zapojení žen, portfolio, udržitelnost aktivit apod.), tzn. podpora *excelentního výzkumu*

Poskytovateli:

- nástroj pro podporu aplikovaného výzkumu a experimentálního vývoje a tím také k dotvoření systému komplementárních programů, pokrývajícího celou škálu technologického vývoje od konceptu k testování a certifikaci (na tento program lze navázat skrze potřeby v SecPro nebo vlastní návrhy v SECTECH)
- možnost sběru námětů, vycházejících především z kreativity výzkumné a inovační sféry a tím diverzifikaci portfolia podpořených projektů za rámec okamžitých nebo krátkodobých potřeb konečných uživatelů
- nástroj pro podporu periferních, přesto důležitých témat, s výrazně širším spektrem potenciálních uživatelů (města, občané, provozovatelé infrastruktur…)

# 4 Členění na podprogramy

Program je členěn na 3 podprogramy, které reprezentují podmnožiny priorit MKBV2017+ při současné reflexi priorit platných strategických a koncepčních dokumentů bezpečnostní politiky (včetně jejich aktualizací po roce 2017), výstupy z průzkumu poptávky ve výzkumné sféře a v neposlední řadě také vysoce specializovaných silných stránek komunity BV v ČR, která se za dobu existence těchto podpor vytvořila.

## 4.1 Podprogram 1: Rozvoj schopností vymáhání práva

### 4.1.1 Očekávané přínosy podprogramu 1

Podprogram přinese cílené zaměření pozornosti žadatelů na priority MKBV2017+ „Efektivní zásah“ a „Adaptabilní bezpečnostní systém“ v oblasti boje proti organizovanému zločinu a dalším závažným formám kriminality, s důrazem na priority Koncepce rozvoje Policie ČR a dalších souvisejících dokumentů. Tyto hrozby i schopnosti, nasazované v rámci boje proti nim se od další činnosti bezpečnostních sborů výrazně liší, jsou charakteristické neustále se adaptujícím oponentem a vysokou mírou inovace na jeho straně. Zároveň reprezentují značnou část inovační poptávky policie (a dalších bezpečnostních sborů).

V rámci bezpečnostní politiky vynikají následující zájmové oblasti, reprezentující jádro poptávky konečných uživatelů výsledků, a tedy i žádoucí oblasti přínosu projektů:

- Forenzní zkoumání, které je dlouhodobě páteří vyšetřování prakticky všech druhů kriminality (cíl A)
- Adaptace na trendy závažné kriminality a zneužívání moderních technologií k jejímu páchání (cíle B – D)
- Analytika, práce s informacemi a efektivní vytěžování maximálního spektra informačních zdrojů (cíl E)
- Znalostní a technologická základna pro inovace ve vyšetřování prioritizovaných typů závažné trestné činnosti (cíle F – I)

### 4.1.2 Cíle a zaměření podprogramu 1

(A) Moderní nástroje forenzního zkoumání napříč obory
(B) Technologie a znalosti pro adaptaci na zneužívání moderních technologií k páchání trestné činnosti a pro online vyšetřování
(C) Technologie a znalosti pro odhalování a prokazování speciálních typů organizované trestné činnosti, zejm. environmentální kriminality, padělání a ilegálního obchodu s uměním nebo předměty kulturního dědictví či s dalšími kvazikomoditami
(D) Technologie pro prvosledové jednotky, zásahové a speciální jednotky
(E) Strategická, taktická a kriminální analýza a metody práce s informacemi, včetně nástrojů jejich získávání a zpracování ze širokého spektra zdrojů
(F) Technologie a znalosti k odhalování a prokazování kybernetické kriminality
(G) Technologie a znalosti k odhalování a prokazování obchodu s drogami
(H) Technologie a znalosti k odhalování a prokazování korupce a hospodářské kriminality
(I) Technologie a znalosti k odhalování a prokazování nelegální migrace a obchodu s lidmi

### 4.1.3 Finanční alokace na podprogram 1

**Finanční alokace na podprogram 1 činí 30% celkových nákladů programu v každém roce.**

## 4.2 Podprogram 2: Krizová připravenost bezpečnostních a záchranných sborů

### 4.2.1 Očekávané přínosy podprogramu 2

Podprogram přinese cílené zaměření pozornosti žadatelů na priority MKBV2017+ „Efektivní zásah“ a „Adaptabilní bezpečnostní systém“ v oblasti krizové připravenosti bezpečnostních a záchranných sborů s důrazem na priority rozvojových dokumentů v oblasti krizového řízení a ochrany obyvatelstva.

V rámci bezpečnostní politiky vynikají následující zájmové oblasti, reprezentující jádro poptávky konečných uživatelů výsledků, a tedy i žádoucí oblasti přínosu projektů:

- Zvládání přírodních katastrof, průmyslových havárií a dalších incidentů s potenciálně vysokým počtem obětí (cíle A – C)
- Problematika efektivního nasazování a ochrany sil a prostředků bezpečnostního systému (cíle D-F)
- Služební příprava a výcvik napříč schopnostmi bezpečnostních a záchranných sborů (cíle G – H)

### 4.2.2 Cíle a zaměření podprogramu 2

(A) Technologie a znalosti pro zvládání incidentů s přítomností CBRN látek a/nebo výbušnin
(B) Technologie a znalosti pro zvládání katastrof, průmyslových havárií a incidentů s vysokým počtem obětí
(C) Technologie a znalosti pro vyšetřování požárů a průmyslových havárií
(D) Technologie a znalosti pro sledování a snižování zdravotní zátěže a zdravotních rizik u příslušníků bezpečnostního systému, jak během zásahu, tak dlouhodobě
(E) Technologie a znalosti pro zajištění efektivní dostupnosti služeb bezpečnostního systému a pro operační řízení
(F) Technologie a znalosti pro zvýšení ekonomické efektivity při zajišťování služeb bezpečnostního systému
(G) Výcvikové metody a technologie
(H) Technologie a znalosti pro rozvoj práce se služebními zvířaty

### 4.2.3 Finanční alokace na podprogram 2

**Finanční alokace na podprogram 2 činí 30% celkových nákladů programu v každém roce.**

## 4.3 Podprogram 3: Odolná společnost

### 4.3.1 Očekávané přínosy podprogramu 3

Podprogram přinese cílené zaměření pozornosti žadatelů na prioritu MKBV2017+ „Resilientní komunity“. Záměrně jde o podprogram charakteristický velkou diverzitou témat, stále ale vychází nebo zahrnují priority strategických a koncepčních dokumentů bezpečnostní politiky. Specificky jsou zahrnuta témata, kde dochází ke značnému překryvu mezi činností bezpečnostního systému, resp. jeho jednotlivých složek s aktivitami dalších aktérů (samosprávy, neziskový sektor, další úřady, občané přímo.). Mezi nejvýznamnější vstupy lze zařadit Koncepci prevence kriminality a odpovídající pasáže Koncepce rozvoje PČR, dále Koncepci environmentální bezpečnosti. I plnění těchto zadání lze vnímat za přínos podprogramu 3.

Rozsah témat odpovídá členění priority „Resilientní komunity“:

- Bezpečná infrastruktura (cíle A-D)
- Bezpečný veřejný prostor (cíle E-I)
- Environmentální bezpečnost (cíle J-L)

### 4.3.2 Cíle a zaměření podprogramu 3

(A) Kyberbezpečnost kritické infrastruktury a klíčových služeb
(B) Fyzická ochrana KI
(C) Bezpečnost a vymáhání práva v dopravě
(D) Bezpečnost a autenticita v dodavatelských řetězcích a ekonomických vztazích
(E) Bezpečnostní aplikace pro chytrá města a regiony
(F) Ochrana měkkých cílů
(G) Právo, etika a soukromí ve vztahu k moderním technologiím ve veřejném prostoru
(H) Prevence kriminality a protispolečenských jevů, zejm. ve vztahu ke zvláště ohroženým skupinám (ženy, děti, senioři), a to jak ve veřejném prostoru, tak v kyberprostoru
(I) Veřejný informační prostor a prevence jeho zneužívání k subverzivním a/nebo kriminálním aktivitám
(J) Snižování negativních dopadů činnosti bezpečnostních a záchranných sborů na životní prostředí
(K) Prevence rizik ekologických katastrof
(L) Naturogenní hrozby, jejich dynamika, vyhodnocování a predikce, včetně vztahu ke klimatické změně

### 4.3.3 Finanční alokace na podprogram 3

**Finanční alokace na podprogram 3 činí 40% celkových nákladů na programu.**

# 5 Financování programu

Celkové výdaje na Program se po dobu trvání předpokládají ve výši cca 2 396 000 tis. Kč podle následujícího rozpisu:

| | *2023* | *2024* | *2025* | *2026* | *2027* | *2028* | *2029* | ***Celkem*** |
|---|---|---|---|---|---|---|---|---|
| ***Veřejné*** | 288 000 | 278 000 | 300 000 | 300 000 | 300 000 | 300 000 | 300 000 | **2 066 000** |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| ***Neveřejné*** | 30 000 | 50 000 | 50 000 | 50 000 | 50 000 | 50 000 | 50 000 | **330 000** |
| ***Celkem*** | 330 000 | 350 000 | 350 000 | 350 000 | 350 000 | 350 000 | 350 000 | **2 396 000** |

**Tabulka 2: Souhrnné finanční ukazatele programu (v tis. Kč)**

Stanovení finančního rámce Programu reflektuje opatření MKBV2017+. Nejvyšší povolená intenzita podpory pro jednotlivé typy podpořených organizací bude určena v souladu s Rámcem a Nařízením a s ohledem na záměr snížit rizika pro poskytovatele u projektů s vyšším komerčním potenciálem.

V případě nedostatečného finančního zajištění bezpečnostního výzkumu jako celku bude poskytovatel postupovat ve smyslu opatření k řízení rizik podle MKBV2017+ a regulovat spektrum témat vyhlašovaných ve veřejných soutěžích.

# 6 Realizace programu

## 6.1 Očekávané výsledky programu

V tomto Programu mohou být podporovány pouze projekty, které odůvodněně předpokládají dosažení alespoň jednoho nového výsledku výzkumu nebo experimentálního vývoje z následujících druhů výsledků, které odpovídají definicím výsledků podle platných předpisů v působnosti Rady vlády pro výzkum, vývoj a inovace a Rejstříku informací o výsledcích platné v době jejich uplatňování.

Za přípustné hlavní výsledky se v tomto Programu považují:

- P – patent;
- G – prototyp a funkční vzorek;
- F – průmyslový a užitný vzor;
- R – software;
- Z – poloprovoz, ověřená technologie;
- N – metodika (všechny podtypy);
- V – výzkumná zpráva obsahující utajované informace;
- S – specializovaná veřejná databáze;
- Výsledky $H_{konc}$
- O – ostatní výsledky, přičemž se pro účely tohoto Programu stanoví následující definice akceptovatelných hlavních výsledků:
    - Výsledky typu S, u nichž nelze, na základě posouzení konečným uživatelem, umožnit veřejný přístup, aniž by byl kompromitován jejich účel v bezpečnostní praxi nebo v dalším výzkumu pro bezpečnostní aplikace a které zároveň nesplňují předpoklady ochrany informací podle zvláštního právního předpisu. Nedílnou součástí výsledku je protokol o převzetí se záznamem o stanovisku konečného uživatele, vč. zdůvodnění omezení veřejného přístupu;
    - „doporučení pro veřejnou správu“ - Doporučení pro veřejnou správu realizuje původní výsledky výzkumu a vývoje, které byly uskutečněny autorem nebo týmem, jehož byl autor členem. Doporučení představuje ucelené, teoreticky a empiricky obhajitelné
      a metodicky přesné návrhy vždy alespoň 3 odlišných variant řešení konkrétně vymezených problémů veřejných politik a metodologicky udržitelné vyhodnocení vhodnosti těchto variant při zavedení do praxe, včetně explicitního zdůvodnění

výběru/doporučení jedné z nich. Nedílnou součástí dokumentu je nezávislý recenzní posudek a protokol o převzetí konečným uživatelem;

Za přípustné vedlejší výsledky se v tomto Programu považují:

- všechny typy hlavních výsledků;
- $V_{souhrn}$ – souhrnná výzkumná zpráva;
- J – recenzovaný odborný článek;
- B – odborná kniha;
- C – kapitola v odborné knize;
- D - stať ve sborníku.

## 6.2 Uchazeči a prokázání jejich způsobilosti

Uchazečem, respektive příjemcem podpory na projekt podle Zákona, Rámce a Nařízení mohou být:

- Organizace pro výzkum a šíření znalostí (VO) – právnické osoby, které splňují definici výzkumné organizace podle čl. 2 odst. 83 Nařízení a dle Zákona, a které řeší projekt ve spolupráci s dalšími účastníky.
- Podniky – právnické i fyzické osoby vykonávající hospodářskou činnost, bez ohledu na právní formu (příloha 1 Nařízení), které řeší projekt samostatně nebo ve spolupráci s dalšími účastníky a prokáží schopnost projekt spolufinancovat z neveřejných prostředků.

Podporu na projekt realizovaný v Programu mohou získat pouze ti uchazeči, kteří splňují podmínky způsobilosti dané § 18 Zákona č. 130/2002 Sb. Uchází-li se o řešení jednoho projektu společně více uchazečů, vztahuje se povinnost prokázat svoji způsobilost na všechny tyto uchazeče.

Způsobilost prokazuje uchazeč doklady dle Zákona způsobem stanoveným poskytovatelem v zadávací dokumentaci.

## 6.3 Intenzita podpory a typologie podpořených projektů

Maximální možná intenzita podpory projektu je stanovena na 100 % uznatelných nákladů. Příjemcům – podnikům, bude poskytována podpora dle Nařízení a příjemcům – výzkumným organizacím, bude podpora poskytována dle Rámce.

**Program podporuje 3 charakteristické typy projektů, v zásadě odpovídající členění na aplikovaný výzkum a experimentální vývoj. Pro každý z uvedených typů se stanoví další limity podpory samostatně, za účelem alespoň částečného sdílení rizika mezi uchazečem a poskytovatelem.**

V rámci tohoto Programu je vyloučeno vyplacení jednotlivé podpory ve prospěch podniku:

- vůči němuž byl v návaznosti na rozhodnutí Evropské komise, na základě kterého/jímž byla podpora obdržená od poskytovatele z České republiky prohlášena za protiprávní a neslučitelnou s vnitřním trhem, vystaven inkasní příkaz, který je nesplacený,
- splňujícímu definici podniku v obtížích uvedenou v čl. 2, odst. 18) Nařízení.

## 6.4 Způsobilé a uznané náklady programu

Podpora bude poskytována na uznatelné náklady projektu vymezené v souladu se Zákonem a Rámcem. Veškeré uznané uznatelné náklady projektu musí být vynaloženy na činnosti přímo související s realizací projektu a musí být přiřazeny na konkrétní kategorie výzkumu a vývoje, tj. na aplikovaný výzkum nebo na experimentální vývoj. Uznatelnými náklady projektu v tomto Programu jsou:

a) osobní náklady nebo výdaje (výzkumných pracovníků, technických pracovníků a ostatního podpůrného personálu) v rozsahu nezbytném pro účely řešení projektu;

b) náklady nebo výdaje na pořízení hmotného majetku v rozsahu a na období, kdy je využíván pro výzkumný projekt; pokud není hmotný majetek využíván pro projekt po celou dobu jeho životnosti, jsou za uznané náklady považovány pouze náklady na odpisy odpovídající délce trvání projektu vypočtené pomocí zavedených účetních postupů;

c) náklady nebo výdaje na pořízení nehmotného majetku nezbytného pro řešení projektu (technické poznatky, patenty, software);

d) další provozní náklady nebo výdaje vzniklé v přímé souvislosti s řešením projektu (např. materiál, drobný hmotný majetek);

e) náklady nebo výdaje na služby vzniklé v přímé souvislosti s řešením projektu (např. sběr dat);

f) doplňkové náklady nebo výdaje vzniklé v přímé souvislosti s řešením projektu (např. režijní náklady, administrativní náklady);

g) pro malé a střední podniky a pro výzkumné organizace náklady nebo výdaje na získání a uznání práv k průmyslovému vlastnictví, které je výsledkem projektu.

## 6.5 Způsob a kritéria hodnocení projektů

Návrhy projektů jsou komplexně hodnoceny v souladu s platnými právními předpisy, především Zákonem. Pro hodnocení návrhů projektů přijatých do veřejné soutěže ustaví poskytovatel odborný poradní orgán. Každý návrh projektu bude hodnocen nejméně dvěma odbornými posudky nezávislých oponentů. Po vyhodnocení splnění podmínek způsobilosti a formálních náležitostí komisí pro přijímání návrhů projektů bude posuzován soulad cílů předložených návrhů projektů s podmínkami Programu.

Kritéria, která budou uplatněna při hodnocení návrhů projektů, jsou:

1) Vylučovací – splnění podmínek veřejné soutěže tohoto Programu
2) Bodovací:
   a) proveditelnost projektu,
   b) nastavení managementu projektu (včetně hodnocení zapojení juniorních výzkumníku a zapojení žen do projektu[13]),
   c) financování projektu,
   d) kvalita výsledků,
   e) očekávaný přínos a implementační potenciál předpokládaných výsledků projektu.

Podrobnější informace o podmínkách pro předložení návrhů projektů, způsobu a kritériích jejich hodnocení budou součástí zadávací dokumentace k jednotlivým vyhlášeným veřejným soutěžím v Programu. Projekty budou hodnoceny dle uvedeného postupu v zadávacích dokumentacích, u každého projektu bude stanoven minimálně jeden závazný výsledek, který bude směřovat k naplnění minimálně jednoho dílčího cíle Programu a tím přispěje k naplňování hlavního cíle Programu.

Odborný poradní orgán (Rada Programu) bude složen nominačním procesem především ze zástupců bezpečnostních a záchranných sborů a ústředních orgánů státní správy, které plní úkoly v oblasti vnitřní bezpečnosti, kteří budou doplněni civilními experty, převážně zástupci profesních asociací,

[13] Vzhledem k tomu, že primárním cílem Programu není podpora juniorních výzkumníků ani podpora zapojení žen do výzkumu, bude toto bodovací kritérium navázáno na stávající bodovací kritéria, které MV uplatňuje, případně ohodnoceno formou bonifikace, přičemž toto bude upraveno v zadávacích dokumentacích pro jednotlivé veřejné soutěže. Kromě toho je nutné upozornit, že bezpečnostní výzkum jako takový je specifickou a svébytnou agendou, kde jsou tato kritéria jen velmi obtížně splnitelná.

působících v oblasti bezpečnosti. Bude tedy mít převážně uživatelský charakter ve smyslu MKBV2017+[14]. Všechny procesy související s hodnocením návrhu projektů, monitorováním projektů a kontrolní procesy jsou poskytovatelem nastavovány tak, aby výzkum prováděný v rámci podpořených projektů přispíval a dosahoval excelentního výzkumu.

# 7 Rizika

V rámci přípravy Programu byla provedena také komplexní analýza rizik spojených s jeho realizací. V níže uvedených tabulkách jsou zaznamenána rizika, která by mohla zamezit nebo omezit dosažení vytyčených cílů. Rizika jsou rozdělena do skupin rizik politických, ekonomických, společenských, technických, legislativních a environmentálních (analýza PESTLE). Žádné environmentální riziko nebylo identifikováno. V analýze byla využita pětistupňová škála hodnocení pravděpodobnosti a dopadu.

Hodnocení jednotlivých rizik vychází z následující tabulky. U každého rizika jsou navržena opatření vedoucí k jeho minimalizaci.

| DOPADY RIZIKA | | | | | | |
|---|---|---|---|---|---|---|
| | **5** | 5 | 10 | 15 | 20 | 25 |
| | **4** | 4 | 8 | 12 | 16 | 20 |
| | **3** | 3 | 6 | 9 | 12 | 15 |
| | **2** | 2 | 4 | 6 | 8 | 10 |
| | **1** | 1 | 2 | 3 | 4 | 5 |
| | | **1** | **2** | **3** | **4** | **5** |
| | | PRAVDĚPODOBNOST VÝSKYTU RIZIKA | | | | |

| VÝZNAM RIZIKA |
|---|
| VYSOKÝ |
| STŘEDNÍ |
| NÍZKÝ |

Tabulka 3: Matice hodnocení rizik

| Riziko | Pravděp. | Dopad | Význam | Popis | Opatření |
|---|---|---|---|---|---|
| **Nerespektování *MKBV2017+* a jejích východisek (řada dalších dokumentů)** | **4** | **4** | vysoký | Program vytváří s ostatními nástroji synergickou soustavu. Ne všechna témata jsou vhodná do všech programů. Souhra mezi tématy a cíli programu je nezbytnou součástí fungování celého systému. To předpokládá MKBV2017+, ale tradiční pohled na „priority“ nikoliv. | Priority MKBV2017+ představují široký konsensus uživatelské sféry. MKBV2017+ dále předpokládá implementaci podpůrných analytických procesů ve spolupráci s externími partnery. MKBV2017+ a na ní navazující produkce je tak jediným hodnověrným zdrojem priorit BV; MV bude aktivně sledovat vývoj v politice VaVaI a snažit se aktivně reprezentovat téma bezpečnosti a jeho specifik (tedy bude volit zcela opačný postup, než v případě Strategie AI). |

[14] V souladu s § 13 a § 21 zákona

| | | | | | |
|---|---|---|---|---|---|
| **Nezájem nebo neaktivita konečných uživatelů v projektech** | **2** | **5** | nízký | Program je striktně závislý na dlouhodobém zapojení konečných uživatelů. Jejich zapojení je nutné od schvalování po provoz projektů. | Přes omezené kapacity konečných uživatelů existuje pozitivní motivace k podpoře projektů, které jsou zacíleny přímo na jejich potřeby, proto se předpokládá vyhlašování i konkrétních potřeb uživatelů. |
| **Nerespektování odbornosti poskytovatele při změnách *Národních priorit* a obdobných dokumentů** | **3** | **4** | střední | Program směřuje k plnění prioritních témat MKBV2017+. Ta shrnují veškerý dostupný materiál bezpečnostní politiky. Pro vědní politiku musí být MKBV2017+ východiskem. Ex post změny a vynucování jiného obsahu učiní program rychle irelevantním. | V případě, že vývoj politiky VaVaI učiní Program irelevantním, bude ukončen nebo přepracován. |

Tabulka 4: Politická rizika Programu

| Riziko | Pravděp. | Dopad | Význam | Popis | Opatření |
|---|---|---|---|---|---|
| **Pokračující relativní finanční propad BV vůči SR VaVaI** | **4** | **4** | vysoký | Dlouhodobý propad financování BV relativně k ostatním problematikám aplikovaného výzkumu snižuje jeho konkurenceschopnost při získávání participace kvalitních organizací. | Program je součástí plnění MKBV2017+, která stanoví opatření pro případ propadu relativního zajištění BV proti SR VaVaI, a to v kapitole F. 1.2, která stanoví, že při propadu podílu BV bude v navazujících výzvách omezován tematický rozsah veřejných soutěží. |
| **Nestabilita finančního zajištění *Programu*** | **4** | **4** | vysoký | Výrazné výkyvy ve financování mohou zlikvidovat veškerý potenciální přínos. Nemožnost zavedení zálohy pro řízení rizik tuto situaci ještě prohlubuje. | Mimo kontrolu poskytovatele, limitně lze výkyvy saturovat z NNV, které ale samy nejsou stabilním a předvídatelným nástrojem k řízení rizika. |
| **Nevyvážené rozpočty ve vztahu k synergickým aktivitám** | **3** | **3** | nízký | Programy definované MKBV2017+ jako synergické vznikají postupně a bez okamžité provázanosti, odhady absorpčních kapacit a nákladů na programy tak mohou být nevyvážené | Poskytovatel předpokládá revizi celého portfolia programů v momentě jejich schválení a následně prvotní implementace v rámci procesů revize a hodnocení plnění MKBV2017+ - v případě, že se toto riziko materializuje, budou programy novelizovány a nastaveny nové poměry financování |
| **Neodpovídající** | | **2** | **3** | Program staví na | Program zahrnuje opatření pro |

| | | | |
|---|---|---|---|
| **odhad absorpční kapacity, resp. výkyvy v projektové nabídce ve vztahu k celkové nebo k dílčím alokacím programu** | dlouhodobých zkušenostech s podporou v tomto segmentu, přesto se lze domnívat, že dojde k výkyvům poptávky (díky nedostatku jiných finančních zdrojů) nebo díky změnám v bezpečnostním či technologickém prostředí | případnou částečnou korekci podle poptávky v rámci realizace veřejných soutěží. V případě razantních výkyvů lze korigovat v rámci zákonného limitu také mezi programy.<br>V případě radikální proměny celého systému poskytování veřejné podpory lze programové portfolio revidovat a znovu nastavit. |

Tabulka 5: Ekonomická rizika Programu

| Riziko | Pravděp. | Dopad | Význam | Popis | Opatření |
|---|---|---|---|---|---|
| **Nezájem o nabízená témata** | **2** | **3** | nízký | Nízká předpokládaná ochota k financování vede k selekci skutečně těch nejvíce specializovaných témat, což značně snižuje potenciál k rekrutaci většího počtu kvalitních kandidátů a ke skutečné soutěži. | Program je v tuto chvíli koncipován tak, aby cílil na témata, která disponují relativně velkou a aktivní komunitou v rámci výzkumné sféry. Zároveň jde o Program otevřený, který k omezení tohoto rizika otevírá možnost přihlášky mimo hlavní témata. |
| **Konkurence méně specifických a otevřenějších tematických oblastí u méně specializovaných pracovišť** | **2** | **3** | nízký | Zatímco specializovaná podstata BV a klesající relativní financování vedou k zužování prioritizovaného pole BV, u ostatních poskytovatelů probíhá opačný proces. To zvyšuje úspěšnost a snižuje transakční náklady pro účast při stejném celkovém absorpčním limitu ze strany uchazečů. | Program do budoucna předpokládá snahu o zajištění vyšší úspěšnosti žádostí. Úspěšnost ovlivňují 2 proměnné, (A) kvalita projektů, (B) dostupné financování. Informační kampaň před výzvami umožňuje rekrutovat kvalitní uchazeče; financování programu tak snadno řídit nelze, přesto se předpokládá, že Program bude jedním z programů určených k absorpci zbytkových financí z ostatních programů (v rámci zákonných limitů). |

Tabulka 6: Společenská rizika Programu

| Riziko | Pravděp. | Dopad | Význam | Popis | Opatření |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| **Číselníky a datová struktura pro přihlášky (IS)** | **2** | **2** | nízký | Program vyžaduje odlišné kategorizace ve srovnání s dosud realizovanými nástroji podpory BV. | Nízké riziko, nutno pouze monitorovat a regulovat manažerskými opatřeními. Je pochopitelné, že rozdílné programy přináší rozdílné kategorizační nároky. |
| **Vzorové smlouvy a programové procesy od začátku** | **2** | **2** | nízký | Některé podprogramy vyžadují nové vzorové smlouvy a procesy. Program je však mechanikou podobný standardním veřejným soutěžím, a proto je riziko nižší než u zcela odlišných programů. Učení ze zkušeností je součástí návrhu. | Nízké riziko, nutno pouze monitorovat a regulovat manažerskými opatřeními. |

Tabulka 7: Technická rizika Programu

| Riziko | Pravděp. | Dopad | Význam | Opatření | Opatření |
|---|---|---|---|---|---|
| **Novela z. 130/2002 Sb. nebere v úvahu mise specializovaných poskytovatelů** | **2** | **2** | nízký | Zcela nepředvídatelný přístup k novele výzkumné legislativy může zcela změnit fungování systému, možnosti poskytovatelů, potenciálně mechanismy projektů atd. | Nutno monitorovat, nelze však formulovat preventivní opatření. V případě zásadních změn a jejich platnosti pro programy schválené před změnou legislativy bude nutné zvážit reformulaci programu a jeho vnitřní mechaniky. |

Tabulka 8: Právní rizika Programu

# 8 Parametry a kritéria hodnocení programu

Jako v případě předchozích programů bezpečnostního výzkumu, je i v tomto případě evaluační strategie výrazně ovlivněna zaměřením na bezpečnostní přínosy z implementace výsledků projektů a soutěžním charakterem a související nepředvídatelností výsledného zaměření portfolia podpořených projektů.

Veškerá realizovaná hodnocení mají proto především formativní cíle. Od průběžně realizovaných vyhodnocení zkušeností, přes průběžný monitoring dosažení základních parametrů Programu po hodnocení závěrečné. Tomu odpovídá jak harmonogram (viz níže), tak skladba indikátorů. V souladu s požadavky MKBV2017+ se programová hodnocení soustředí především na zjišťování jeho funkčnosti, efektivity a relevance.

Ze soutěžního a otevřeného charakteru programu plyne také nutnost sledovat indikátory popisného charakteru, které neposkytují základ pro normativní výroky o hodnocených vlastnostech programu, ale dokumentují, kam podpora z programu mířila. Je nutno mít na paměti, že poskytovatel je ve veřejné soutěži především moderátorem a má jen limitní vliv na spektrum přihlášek a konsekventně

také na podpořenou množinu projektů. Pro hodnocení se použije následující soustava evaluačních otázek, pro průběžné hodnocení se použije pouze relevantní část:

| Sekce | Hodnotí | Otázka | Indikátory |
|---|---|---|---|
| Implementace programu | Funkčnost | Jsou realizovány veřejné soutěže a projekty? | Milníky realizace, indikátory funkčnosti programu, vývoj rozpočtu |
| | | Je program adekvátně finančně zajištěn? | Rozpočtová alokace v letech; řízení finančních alokací pro programy podle poptávky; spoluúčast příjemců |
| | | Jsou používané metody výběru projektů správné?[15] | Výběrové postupy podle zákona, podle programu, výstupy z hodnocení, chybovost přihlášek |
| | | Je podpora předpokládaným způsobem diverzifikovaná? | Obory v programu, subjekty v programu, zastoupení věcných priorit[16], zastoupení uživatelských organizací mezi odbornými gestory |
| | | Je správně prováděno monitorování projektů? [17] | Kontrolní činnost v souladu s legislativou, výstupy kontrolní činnosti |
| Cíle programu | Efektivita | Jaká je stávající míra naplnění cílů? | Minimální počty projektů a výsledků podle indikátorů efektivity programu |
| | | Jaké jsou ekonomické parametry programu? | Podpořená pracovní místa, přímo zpět do SR, financování infrastruktury (využití kapacit v projektech) |
| | | Jaká je efektivita programu z hlediska předpokládaných výstupů? | Kvalita výsledků programu, hodnocení ukončených projektů |
| | | Jaký je bezpečnostní přínos výsledků programu? | Statistika hodnocení uživatelského přínosu výsledků podle priorit MKBV2017+ a podle zájmových oblastí BV |
| Další charakteristiky programu | Relevance | Mají podané návrhy projektů ambice naplnit cíle Programu? [18] | Zastoupení cílů a témat v přihláškách a na podpoře, přihlášky mimo BV, počet projektů v oblasti environmentální bezpečnosti[19] |

[15] Podle UV č. 351/2015.

[16] Podle UV č. 569/2013 k Implementaci Národních priorit orientovaného výzkumu, vývoje a inovací

[17] Podle UV č. 351/2015.

[18] Podle UV č. 351/2015.

[19] Nutno měřit ve vztahu k úkolu KEB2021+

| | | | |
|---|---|---|---|
| | | Je program relevantní z hlediska portfolia bezpečnostního výzkumu? | Zaměření projektů ve srovnání s programy IP, SecPro, SECTECH a IMPAKT, účast příjemců IP a resortních organizací MV |
| | | Jaký je ohlas příjemců podpory? | Převis poptávky, přínosy z účasti pro podpořené organizace (internacionalizace, rozvoj lidských zdrojů, networking), spokojenost partnerů |
| | | Obsahuje program jednoznačnou vazbu na RIS3 strategii?[20] | Zaměření projektů |
| | | Zahrnuje program podporu rozvoje lidských zdrojů, zejména mladé generace? [21] | N/A – program není zacílen tímto směrem |
| | | Podporuje program spolupráci průmyslové a akademické sféry?[22] | Charakter spolupráce, intenzita zapojení jednotlivých typů aktérů, účast podniků podle typů ve spolupráci, přítomnost spin-off firem |
| Závěr hodnocení a úprava programu | | Jaká opatření je vhodné udělat pro prohloubení funkce, efektivity a relevance programu? | Proces učení ze zkušeností |

Tabulka 9: Koncept závěrečného hodnocení programu

## 8.1 Harmonogram hodnocení

Tato kapitola shrnuje harmonogram hodnotících procesů Programu[23], resp. harmonogram vydávání hodnotících materiálů. Tento plán nepředstavuje závazné milníky, neboť tyto jsou závislé na přesných datech konání veřejných soutěží a ukončování projektů z jednotlivých výzev. Návrh ale v maximální míře zohledňuje praktické limity implementace Programu.

| *rok* | **Aktivita** | **Výstup** | **vlastník** |
|---|---|---|---|
| *2022* | Hodnocení zkušeností VS1 | Modifikace procesů VS | MV |
| *2024* | Hodnocení zkušeností VS2 | Modifikace procesů VS | MV |
| *2025* | Hodnocení zkušeností VS3 | Modifikace procesů VS | MV |
| *2026* | Závěrečné hodnocení projektů VS1 | | MV |
| | Průběžné hodnocení Programu | Podklad pro tvorbu navazujícího programu | MV |

[20] Nutno hodnotit v návaznosti na jednání k rozpočtu 2022+.

[21] Nutno hodnotit v návaznosti na jednání k rozpočtu 2022+.

[22] Nutno hodnotit v návaznosti na jednání k rozpočtu 2022+

[23] Hodnocení programu (včetně parametrů programu jako je charakter a využití výsledků programu, splnění cílů programu, plnění NPOV, oborové zaměření, čerpání finančních prostředků aj.) bude provedeno v souladu s UV č. 351/2015 a v souladu s UV č. 107/2017

| | | | |
|---|---|---|---|
| *2027* | Závěrečné hodnocení projektů VS2 | | MV |
| *2030* | Závěrečné hodnocení projektů VS3 | | MV |
| *2030* | Závěrečná zpráva o Programu | Uzavření programového cyklu. Závěrečnou zprávu o Programu zpracuje MV v rozsahu podle Metodiky hodnocení výzkumných organizací a výsledků ukončených programů schválené vládou | RVVI |
| *2030* | Hodnocení dopadů projektů VS1 | Vstup do hodnocení dopadů programu | Ext[24] |
| *2031* | Hodnocení dopadů projektů VS2 | Vstup do hodnocení dopadů programu | Ext |
| *2034* | Hodnocení dopadů Programu | Vstup do přípravy meziresortní koncepce bezpečnostního výzkumu | MV |

**Tabulka 10: Harmonogram hodnotících procesů v Programu**

## 8.2 Funkčnost

Tato podkapitola stanoví základní minimální prahy pro hodnocení funkčnosti Programu, které budou předmětem hodnocení. Je zřejmé, že funkčnost specializovaného Programu ukazuje i řada dalších indikátorů. Pro ně ale zpravidla není možné prahy hodnověrně určit, buď pro nedostatek relevantních empirických vstupů, nebo kvůli **soutěžnímu mechanismu**. Ten **vylučuje jakoukoliv předchozí znalost jak spektra přihlášek, tak spektra podpořených projektů.**

| Indikátor | Hodnota |
|---|---|
| Rozdíl ve finanční alokaci na Program v letech | ≤ 10 % |
| Minimální čerpání rozpočtu v letech | 70 % |
| Realizace finančních kontrol v roce | ≥ 5% poskytované podpory |
| Odchylky v harmonogramu vyhlašování veřejných soutěží | max 1 rok |
| Úspěšnost žádostí za dobu realizace Programu | ≥ 20 % |
| Milníky harmonogramu hodnocení Programu | v termínu |

**Tabulka 11: Hodnocení funkčnosti Programu**

## 8.3 Efektivita

Tato podkapitola shrnuje základní prahové hodnoty pro sledování efektivity Programu. Je zřejmé, že pro její detailní vyhodnocení je vhodné systém vyhodnocování minimálního plnění doplnit o další, zpravidla kvalitativní indikátory. Protože je Program realizován veřejnou soutěží a poskytovatel tak dopředu nezná ani složení přihlášek, ani složení množiny podpořených projektů a tuto otevřenost se snaží zachovat, neklade si žádné předběžné ambice z hlediska diverzity podpořených projektů.

| **Indikátor** | **Hodnota** |
|---|---|
| Minimální počet podpořených projektů | 100 |

[24] Dosavadní vývoj v přípravě tzv. Metodiky hodnocení programů a platná usnesení vlády k této problematice předpokládají realizaci těchto hodnocení externě.

| | |
|---|---|
| Minimální podíl úspěšně ukončených projektů | 80 % |
| Maximální podíl výsledků hodnocených jako D[25] | ≤15 % |
| Minimální podíl výsledků hodnocených jako A nebo B | ≥15 % |

Tabulka 12: Hodnocení efektivity Programu

## 8.4 Relevance

Stejně jako v případě hodnocení efektivity, platí i u hodnocení relevance Programu, že základní minimální prahy lze stanovit pouze pro některé indikátory. Soutěžní povaha tohoto instrumentu potom vyžaduje i řadu deskriptivních indikátorů, jejichž hodnoty nelze predikovat.

| Indikátor | Hodnota |
|---|---|
| Vazba na NPOV | všechny projekty relevantní |
| Vazba na RIS3 | všechny projekty relevantní |
| Vazba na NP VaVaI | všechny projekty relevantní |
| Synergie s ostatními programy podpory BV | nedochází k duplicitám[26] |
| Minimální podíl juniorních výzkumníků[27] | ≥ 20 % |
| Minimální zastoupení žen | ≥ 26 % [28] |

Tabulka 13: Hodnocení relevance Programu

## 8.5 Dopady

Tematické okruhy hodnocení dopadů jsou voleny s důrazem na očekávané přínosy Programu a jsou členěny do 6 následujících kapitol: potenciál pro rozvoj zkoumaného tématu/oblasti, další výzkumné aktivity (navazující spolupráce, ocenění spojená s projektem aj.), popularizace v komunitě (konferenční činnost, neakademická komunita, mediální prezentace aj.), vzdělávání (akademické vzdělávání, profesní příprava aj.), bezpečnostní politika (legislativní/nelegislativní předpisy, koncepční a strategické materiály, programy a evaluace.) a produkty (licenční využití výsledků, výroba, spin-off, navazující služby aj.).

Jedinou hodnověrnou metodou pro sledování tohoto typu dopadů jsou případové studie. Vzhledem k předpokládanému počtu projektů se předpokládá realizace případových studií u reprezentativního vzorku podpořených projektů. Ty by měly přinést zásadní formativní vstupy pro plánování dalších kol Programu i z projektů, kde implementace neprobíhá úspěšně.

V rámci realizace hodnocení se předpokládá každoroční interakce s podpořenými subjekty formou řízených dotazníků, které také představují hlavní zdroj dat pro hodnocení. Hodnotící zpráva bude vytvořena 4 roky po ukončení Programu, tj. rok po vyhodnocení období udržitelnosti projektů z posledního běhu Programu.

| Otázka | Indikátor | Metoda |
|---|---|---|
| Jsou výsledky šířeny mezi uživatelskou | Implementace výsledků | Mapování implementace |

[25] Odstupňování hodnocení výsledků programových projektů přímo vychází z konceptu Metodiky hodnocení výsledků výzkumných organizací 2017+

[26] Navazující financování se za duplicitu nepovažuje, naopak, jedním ze znaků relevance Programu by měl být přechod některých výsledků jiných finančních nástrojů do tohoto Programu

[27] Program primárně necílí na zapojení juniorních výzkumníků ani na genderovou otázku, veličina je sledována v návaznosti na aktuální trendy v této oblasti

[28] European Commission DG Research and Innovation (2015) She Figures 2015: Gender in Research and Innovation – Statistics and Indicators. Brussels: EU Publication Office

| | | |
|---|---|---|
| komunitu? Jak? | (společenský dopad) | (dotazníkové šetření, každoroční) |
| Kdo používá aplikované výsledky a k čemu přispěly? | Využití aplikovaných výsledků | Případové studie na vzorku výsledků |
| Jaký je vliv Programu na další vývojovou aktivitu? | Navazující projekty, předcházející projekty bez ohledu na zdroj | Relační analýza |

**Tabulka 14: Hodnocení dopadů Programu**